UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Tadej Markun

RAZVOJ VAJ ZA UČENJE UPORABE STIKALA NASLEDNJE GENERACIJE

DIPLOMSKO DELO

VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana, september 2014

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Preučite predstavnika stikal naslednje generacije, ki poleg prepošiljanja okvirjev poznajo še številne omrežne funkcije in varnostne mehanizme. Najprej v teoriji pojasnite omrežne koncepte, ki jih je potrebno razumeti za uporabo te funkcionalnosti, nato pa zasnujte sistem vaj z rešitvami, ki se medsebojno nadgrajujejo in bi jih lahko uporabljali inženirji za učenje uporabe tovrstnih naprav v virtualnih laboratorijih. Pojasnite tudi naprednejše koncepte, na primer pregledovanje šifriranega prometa, in komentirajte legalnost takšne aktivnosti. Komentirajte doprinos vašega diplomskega dela za uporabo v podjetju, ki se ukvarja z izobraževanjem s področja računalniških tehnologij.

IZJAVA O AVTORSTVU

diplomskega dela

Spodaj podpisani Tadej Markun, z vpisno številko 63030251, sem avtor diplomskega dela z naslovom:

Razvoj vaj za učenje uporabe stikala naslednje generacije

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojca Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 25. september 2014 Podpis avtorja:

Zahvaljujem se mentorici, doc. dr. Mojca Ciglarič, za pomoč in potrpežljivost.

Zahvaljujem se vsem, ki so mi omogočili tehnično, programsko in strojno opremo, stali ob strani ali mi kakorkoli pomagali.

Najbolj pa sem hvaležen staršema, ki sta mi omogočila, da se postal to, kar sem.

Kazalo

Kazalo tabel

Kazalo slik

Povzetek

Diplomsko delo obsega predstavitev in nastavitev požarne pregrade Palo Alto naslednje generacije. Cilj diplomske naloge je bralcu, ki ima potrebno opremo, željo po nastavitvi požarne pregrade Palo Alto in je računalniško pismen, s pomočjo nalog podati ključno znanje in novosti, ki jih prinaša požarna pregrada zadnje generacije.

Teoretični in izvedbeni del (deli, podani z nalogami) bralca smiselno vodita do nastavitve požarne pregrade Palo Alto. Naloge obsegajo umestitev požarne pregrade v lokalno omrežje, priprave vmesnikov, varnostnih pravil in preslikovalnega pravila, prepoznavanje groženj ter prepoznavanje in blokiranje aplikacij ter dešifriranje prometa, torej funkcionalnosti, ki jih potrebujemo za nastavitev za dobro zaščito. Naloge so umeščene v posamezna poglavja, ki se vsebinsko navezujejo na teoretični del.

S pridobljenim znanjem in rešenimi nalogami bo bralec prišel do smernic za uspešno nastavitev požarne pregrade. To mu bo omogočilo osnovno varnostno higieno za varno zaščito lokalnega omrežja. Za lažje razumevanje nalog ima bralec podane rešitve nalog, ki se nahajajo ob koncu diplomske naloge.

Predstavljene naloge, ki jih bo bralec obdelal, pa obsegajo le peščico možnosti nastavitev, ki jih požarna pregrada Palo Alto ponuja. Diplomska naloga je tako odskočna deska za poglobljeno študijo požarne pregrade Palo Alto.

Ključne besede: požarna pregrada , Palo Alto, požarna pregrada naslednje generacije

Abstract

The dissertation includes presentation and configuration Palo Alto firewall, firewall of next generation. The aim of dissertation is to provide essential knowledge and innovations, which are brought by the firewall of the latest generation. Reader needs to have the equipment, desire to learn about firewall Palo Alto and has basic computer knowledge.

Reader is guided through the part with theory and exercises. The exercises include placing firewall into local network, configuration of interfaces, configuration security policies, configuration translation policies, threat and application recognition, blocking application and decrypt traffic. These are the steps needed for setting the firewall and wanted protection. You can find exercises in individual chapters, which are thematically similar to parts where theory is presented.

By reading this dissertation and exercises reader gets essential guidelines for successful firewall preparation. Configuration firewall gives him basics for local network protection. At the end of dissertation you can find solutions to each exercise.

Exercises in dissertation include only few functionalities of firewall Palo Alto. That is why dissertation can be an important part of further study of Palo Alto firewall.

Keywords: firewall, Palo Alto, next generation firewall

1. Uvod

Živimo v času, ko je dostop do interneta nekaj vsakdanjega. Vsakodnevna uporaba spleta ponuja nove možnosti za nove ideje. Ker se vsak dan na spletu pojavljajo nove vsebine, lahko rečemo, da je splet postal izredno bogata knjižica znanj, žal pa tudi groženj. V zadnjem času smo priča naraščajočemu trendu selitve aplikacij na svetovni splet, pri tem pa ne smemo zanemariti posledic, ki ob tem nastajajo, zlasti iz vidika varnosti. Čeprav internet štejemo kot dobro, tisto, kar nam omogoča (hiter) dostop do želenih vsebin in znanj, po drugi strani predstavlja tudi nevarnost, ki se je še vedno premalo zavedamo.

Povečanje groženj in verjetnosti za vdor ter krajo podatkov, tudi intelektualne lastnine, sproža vprašanje varnosti, po drugi strani pa tudi ozaveščanje ljudi o varnosti njihovih podatkov. Marsikdo sicer pomisli, da na svojem računalniku ne hrani ničesar vrednega, zato se morebitnega vdora ne boji, a njihovo razkritje vedno znova pokaže, da vendarle so vredni. Dober primer »nič vrednih« podatkov je vsakoletno poročanje medijev o kraji fotografij in drugih zasebnih podatkov zvezdnikov, ki so ukradeno lastnino hranili bodisi na telefonu, osebnem računalniku ali v oblačnih storitvah.

Uporaba slednjih vse bolj narašča, in sicer tako pri fizičnih kot pri poslovnih uporabnikih, saj lahko prek omenjenih storitev svoje storitve in dokumente, ki so jih prej uporabljali v lokalnih omrežjih, selijo v oblake. S tem je postal pomen varovanja oddaljenih, lahko bi rekel tudi bolj izpostavljenih podatkov, še večji.

Med najbolj učinkovite naprave za varovanje podatkov, obrambo pred zlonamerno ali škodljivo vsebino in vsiljivci štejemo požarne pregrade, ki se nenehno izpopolnjujejo in odpravljajo svoje ranljivosti. Naslednja generacija požarnih pregrad, v katero spada tudi požarna pregrada Palo Alto, trenutno velja za najbolj izpopolnjeno v tej problematiki. Večje zavedanje podjetij in drugih institucij o pomembnosti kakovostne zaščite pred morebitnimi vsiljivci se kaže tudi v porastu prodaje s strani Palo Alta; nedavno je to kalifornijsko podjetje predstavilo podatke za tretje fiskalno četrtletje letošnjega leta in razkrilo rekordne poslovne rezultate. Uporaba omenjene požarne pregrade narašča tudi v Sloveniji, kjer ga trenutno uporablja 50 podjetij, med njimi tudi nekatera večja (trgovinska veriga Interspar).

Moje prvo srečanje s požarnimi pregradami, natančneje z ISA server 2003, sega nekaj let nazaj, zanimanje pa se je nadaljevalo ob najavi požarne pregrade naslednje generacije Palo Alto. Takrat sem spoznal, kakšen razvoj stoji za napravo in česa vse je zmožna narediti. Ob nastopu obdobja za izdelavo diplomske naloge sem se odločil, da napravo Palo Alto pobliže spoznam in jo predstavim še tistim, ki jo potrebujejo za varnejše delovanje.

Prav zato je namen diplomske naloge seznaniti s požarno pregrado vsakogar, ki je željan uporabe požarne pregrade Palo Alto in je računalniško pismen. S pomočjo nalog ga želim pripeljati do ključnega znanja in novosti, ki jih prinašajo požarne pregrade Palo Alto. Namen vaj v diplomski nalogi je tudi možnost izvajanja prek virtualnega laboratorija, in sicer tako, da bi si eno ali nekaj naprav delilo večje število inženirjev.

Za prikaz praktičnih nalog bom uporabil požarno pregrado naslednje generacije Palo Alto VM-300. Oprema, ki sem jo potreboval za izdelavo praktičnega dela, za fizične uporabnike dosega vrtoglave cene. To je ena od težav, na katere sem naletel še pred samim raziskovanjem. Poleg naprave je potrebno za uporabo oziroma za delovanje in izvajanje določenih funkcionalnosti potrebno še plačati licenco, ki dosega polovično ceno naprave. Pravi finančni zalogaj, ki pa se z vidika varnosti še kako izplača.

Teoretični del

2. Standardizacija komunikacije

Da lahko naprave med seboj uspešno komunicirajo, morajo govoriti isti jezik. Proizvajalci so pred vzpostavitvijo standarda ISO OSI uporabljali lastne protokole za komuniciranje med napravami. Naprave so lahko medsebojno komunicirale le, če so poznale protokol. Do vzpostavitve standarda ISO je veljalo, da napravi dveh različnih proizvajalcev nista bili sposobni komunicirati med seboj.

Zaradi zmešnjave v komunikacijskem jeziku je mednarodna organizacija za standardizacijo ISO v začetku osemdesetih let prejšnjega stoletja sprejela mednarodni standard imenovan OSI (ang. Open System Interconnection).

Model ISO OSI je sestavljen iz sedmih nivojev:

- fizičnega ali nivoja 1 (ang. Physical layer ali Layer 1), katerega naloga je povezovanje in prenašanje bitov po komunikacijskem kanalu. Na tem nivoju delujejo razdelilniki (ang. hub), za fizično povezavo pa skrbijo kabli UTP, FTP, optična vlakna itd [27].

- povezovalnega ali nivoja 2 (ang. Data link layer ali Layer 2), ki skrbi za okvirjanje bitov, kontrolo pretoka, popravljanje napak, asinhrono/sinhrono komunikacijo. Na tem nivoju delujejo stikala (ang. switch), mostovi (ang. bridges) in drugo. Protokoli, ki delujejo na tem nivoju, so ARP, IPCP, SLIP, Ethernet, PPTP, PPP, VLAN itd [27].

- omrežnega ali nivo 3 (ang. Network layer ali Layer 3), ki skrbi za usmerjanje, posredovanje, njegova naloga je tudi izogibanje zamašitvam. Na tem nivoju delujejo nekatera stikala in usmerjevalniki (ang. Routers). Protokoli, ki delujejo na tem nivoju, so AppleTalk, IPX/SPX, IP, IPv6, ICMP, ICMPv6, itd [27].

- transportnega ali nivoja 4 (ang. Transport layer ali Layer 4), ki skrbi za zanesljivost in učinkovitost prenosa. Protokoli, ki delujejo na tem nivoju, so TCP, UDP, TALI, RUDP, SPX, itd [27].

- sejnega ali nivoja 5 (ang. Session layer ali Layer 5), ki skrbi za logično povezovanje procesov znotraj aplikacij, aplikacijsko multipleksiranje. Protokoli, ki delujejo na tem nivoju, so RPC, NFS, SMB, SOCKS, itd [27].

- predstavitvenega ali nivoja 6 (ang. Presentation layer ali Layer 6), ki skrbi za kodiranje, dekodiranje in stiskanje podatkov. Protokoli, ki delujejo na tem nivoju TLS, so SSL, LPP, itd [27].

- aplikacijskega ali nivoja 7 (ang. Application layer ali Layer 7), ki skrbi za interakcijo podatkov uporabniku. Protokoli, ki delujejo na tem nivoju so BOOTP, DCAP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAP4, LDAP itd [27].

Protokoli so točno določena pravila, ki omogočajo komunikacijo med isto ležnimi procesi, določajo metodo preverjanja napak, preprečujejo napake, določajo, kako pošiljati in sprejemati protokolarna sporočila. Običajno protokol definira vsa komunikacijska pravila, ki se nahajajo od nivoja 2 do nivoja 7 po ISO OSI modelu.

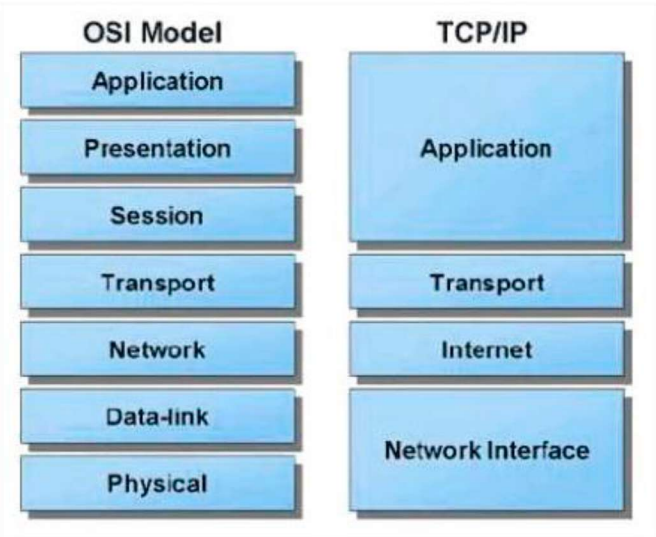
ISO OSI model lahko v grobem razdelimo v dve skupini: na zgornji nivo, v katerega so uvrščeni nivoji od 7 do 5 in spodnji nivo, v katerega so razvrščeni nivoji 4,3,2 in 1. Zgornji nivo sodeluje pri dejanskih podatkih, pri čemer je najvišji, nivo 7, najbližje uporabnikom, medtem ko spodnji nivo skrbi za prenos posredovanih podatkov iz zgornjega nivoja.

OSI modelu bi lahko rekli tudi vodnik skozi razumevanje potovanja informacije od pošiljatelja do prejemnika.

Pri pošiljanju informacij si nivoji sledijo hierarhično od aplikacijskega sloja proti fizičnemu, kar imenujemo enkapsulacija, pri prejemanju informacij v obratnem vrstnem redu pa postopek imenujemo dekapsulacija. Naloga aplikacijskega, predstavitvenega in sejnega nivoja je posredovanje podatkov transportnemu. Za predstavo podatkov iz transportnega nivoja skrbi na primer spletni brskalnik, ki na človeku prijazen način predstavlja podatke. Transportni nivo prejete podatke iz nivojev 7, 6 in 5 (aplikacijskega, predstavitvenega in sejnega) opremi z izvornimi in ciljnimi vrati, jih segmentira in posreduje omrežnemu nivoju. Omrežni nivo prejete podatke opremi z izvornim in ciljnim naslovom, okviri in posreduje povezovalnemu nivoju.

Povezovalni nivo poskrbi, da se podatki prek fizičnega nivoja prenesejo po omrežju. Fizični nivo predstavlja prenosni medij.

Poleg ISO OSI modela obstaja tudi TCP/IP sklad (ang. TCP/IP Stack), ki pa ima v primerjavi z ISO OSI modelom manj nivojev. TCP/IP je zgrajen iz štirih nivojev: aplikacijskega (lahko bi rekel, da združuje 7, 6 in 5 nivo modela ISO OSI), transportnega, ki je enakovreden transportnemu nivoju iz ISO OSI, internetnega, ki je enakovreden omrežnemu nivoju iz modela ISO OSI in omrežnega, ki je enak 1 in 2 nivoju (fizičnemu in povezovalnemu) iz ISO OSI modela [2].



Slika 1 Primerjava nivojske sestave modelov ISO OSI in TCP/IP

Vsaka naprava v omrežju ima dodeljen enoznačen internetni naslov, ki se imenuje IP naslov (ang. IP internet protocol ali IP address). Naprava, ki je priklopljena v omrežje, ima lahko več IP naslovov. Zato pravimo, da IP naslov ni vezan na napravo, ampak na vmesnik na napravi. Vmesnik je programska ali strojna oprema, ki skrbi za povezljivost med dvema napravama [25].

Poznamo dve generaciji IP naslavljanja. Prva, starejša generacija, se imenuje IP različica 4 (IPv4), druga, ki je novejša, pa IP različica 6 (IPv6). IPv4 je 32 bitno število, ki predstavlja dva dela naslova identifikacijskega števila omrežja (ang. network ID) in naprave (ang. host ID) [25].

```
11111111 11111111 11111111 11100000  ali  255.255.255.224
11111111 11111111 11111111 11110000  ali  255.255.255.240
11111111 11111111 11111111 11111000  ali  255.255.255.248
```

Slika 2 Prikaz 32 bitnega zapisa IP naslova (levo), desetiški zapis IP naslova

Zaradi ljudem bližjemu desetiškemu številčenju se različica IPv4 zapisuje v obliki 213.157.249.10. Različica v4 nam ponuja namreč 2^32=4.294.967.296 naslovov, zato je snovalcem že na začetku 90. let prejšnjega stoletja postalo jasno, da bo naslovov kaj kmalu zmanjkalo. V ta namen so razvili različico IPv6, ki nam omogoča 2^{128} unikatnih naslovov zapisanih z 128 bitnim številom [25].

V diplomski nalogi bom uporabljal različico IPv4. Naprava, ki jo uporabljam, sicer omogoča naslavljanje v IPv6, vendar pa bo zaradi lažjega razumevanja bolj uporabna različica IPv4. Za potrebe poznavanja nastavitev je v tem trenutku zadostno poznavanje različice IPv4.

Maska podomrežja določa omrežni segment in lokacijo naprave. Zapisana je z 32 bitnim številom in predstavlja mejo omrežja med omrežjem in podomrežjem.

Za lažje razumevanje naj podam primer: omrežje z masko podomrežja 255.255.255.0 bo lahko naslovilo 254 naprav, v primeru maske podomrežja 255.255.0.0 pa že 65.023 naprav.

2.1. Omrežja WAN

Omrežja WAN (ang. wide area network) predstavljajo tehnologije, ki omogočajo povezovanje na velike razdalje. Organizacija ima lahko eno ali več različnih WAN povezav, ki služijo določenim potrebam. Skozi zgodovino so razvili več različnih tehnologij omrežij WAN.

Med najkakovostnejše trenutno uvrščamo t.i. najete vode, ki predstavljajo povezavo med dvema točkama, so pod polnim nadzorom uporabnika in so rezervirana samo zanj. Pri nas za najbolj razširjene tehnologije priklopa na WAN omrežje veljajo optične povezave in xDSL digitalne naročniške linije, med katere uvrščamo ADSL, VDSL, SHDSL itd.

2.2. Omrežja LAN

V času delovanja in razvoja omrežij so analize pokazale, da približno 80 odstotkov podatkov, ki jih ustvari neka poslovna enota, nikoli ne zapusti njene geografske lokacije, ampak kroži znotraj nje. Zaradi tega so nastala LAN (ang. local area network) omrežja.

LAN namreč temelji na zasnovi istega prenosnega medija, kar pomeni, da si naprave znotraj enote delijo isti prenosni medij, pri čemer prenosni medij predstavlja fizično povezavo med dvema enotama. Danes med najbolj razširjene mrežne prenosne medije štejemo zvito parico (ang. UTP ali twisted pair), brezžično omrežje (ang. WIFI) in optična vlakna (optical fiber).

Ker so se zahteve zaradi multimedijskih aplikacij po pasovni širini začele povečevati, se je arhitektura LAN omrežij začela spreminjati. Tako so omrežne razdelilnike (ang. hub) nadomestila stikala (ang. switch) ali usmerjevalniki (ang. router). Danes velika večina lokalnih omrežij sloni na tehnologiji Ethernet.

2.3. Dodeljevanje enoznačnih IP naslovov

Poznamo dva pristopa za dodeljevanje enoznačnih IP naslovov: statičnega (ang. Static addressing) in dinamičnega (ang. Dynamic addresing). Statično dodeljevanje enoznačnih IP

naslovov temelji na fizični nastavitvi naslova napravi. Ta se ne spreminja, dokler sami ne spremenimo naslov. Uporablja se pri napravah, pri katerih moramo v vsakem trenutku točno vedeti njihov naslov, da bi lahko koristili storitev, ki nam jo nudijo. Med te naprave uvrščamo požarne pregrade, usmerjevalnike, strežnike in druge. Eden največjih problemov statičnega dodeljevanja IP naslovov je, da kaj hitro preidemo v neobvladljive evidence že dodeljenim naslovov napravam, zaradi česar lahko pride do podvajanja naslovov [2].

Med slabosti oziroma pomanjkljivosti bi lahko navedel tudi vzdrževanje in preštevilčenje naslovov napravam, saj je postopek zapleten in časovno zamuden. Zaradi omenjenih slabosti statičnega dodeljevanja enoznačnih IP naslovov se je kmalu pojavilo dinamično dodeljevanje IP naslovov [2].

Tovrstno dodeljevanje omogoča avtomatično dodeljevanje naslovov napravam v omrežju. S tem upravljavcem omrežja ni potrebno več upravljati z zapisi in seznami dodeljenih IP naslovov ter ugotavljati, kateri naslovi so že zasedeni in podobno. Vsaka naprava, ki želi komunicirati v omrežju, mora pridobiti IP naslov. Pri avtomatičnem naslavljanju za to skrbi strežnik, imenovan DHCP (ang. Dynamic Host Configuration Protocol).

DHCP strežnik napravi avtomatično dodeli enoznačen IP naslov, naprava pa uporablja naslov, vse dokler ga ne sprosti oziroma vse dokler ji ne poteče dodeljen čas (ang. lease). Za lažje razumevanje bi si lahko DHCP strežnik predstavljali kot najem avtomobila. Za prevoz iz točke A v točko B potrebujemo vozilo, zato si prevozno sredstvo sposodimo pri avtomobilskem najemodajalcu (DHCP strežnik dodeli nek naslov). Izposojeni avtomobil lahko uporabljamo dokler ne poteče čas najema (ne poteče »lease«) oziroma ga vrnemo najemodajalcu (npr. naprava se izklopi iz omrežja). DHCP strežnik poleg dodeljevanja enoznačnih naslovov napravam hrani tudi zapise o dodeljenih naslovih, kar ji omogoča, da v vsakem trenutku ve, kateri naslov je bil dodeljen, kdaj poteče in katerega lahko promovira v prihodnje.

Kako DHCP strežnik dodeljuje enoznačni IP naslov? Postopek poteka v štirih korakih:

- Prvi korak: DHCP odjemalec pošlje DHCPDISCOVER sporočilo DHCP strežniku.

  DHCPDISCOVER je sporočilo, ki označuje začetek dodeljevanja naslova med odjemalcem in strežnikom. Ker odjemalec še nima IP naslova in ne pozna naslova DHCP strežnika, odjemalec pošlje DHCPDISCOVER sporočilo na vse naslove. To sporočilo ima vedno izvorni naslov 0.0.0.0, ciljni naslov pa 255.255.255.255 [29].

- Drugi korak: Ko DHCP strežnik prejme DHCPDISCOVER sporočilo, mu odgovori z DHCPOFFER sporočilom. Ker odjemalec še nima naslova, je sporočilo poslano na vse naslove (255.255.255.255).

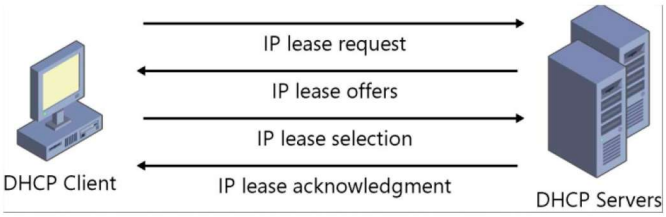
DHCPOFFER je sporočilo, ki je posredovano s strani DHCP strežnika kot odgovor na DHCPDISCOVER in vsebuje nastavitve za dodelitev naslova odjemalcu, ki je posredoval DHCPDISCOVER [29].

- Tretji korak: DHCP odjemalec posreduje z odgovori DHCPREQUEST, pri čemer potrdi prejete nastavitve, poslane z DHCPOFFER sporočilom. V primeru, da je na voljo več DHCP strežnikov, bo odjemalec prejel več DHCPOFFER-jev, s tem, da bo dogovoril samo na enega.

  DHCPREQUEST je sporočilo, odgovor na DHCPOFFER, s katerim potrdi prejete nastavitve, prejete v DHCPOFFER-ju [29].

- Četrti korak: Ko DHCP strežnik prejme DHCPREQUEST od DHCP odjemalca, pošlje potrditveno sporočilo DHCPACK, ki DHCP odjemalcu dovoli uporabo dodeljenega naslova.

  DHCPACK je sporočilo, poslano s strani DHCP strežnika, ki je kot odgovor na DHCPREQUEST poslan s strani DHCP odjemalca. S tem sporočilom se zaključi proces pridobivanja naslova in odjemalec lahko začne uporabljati nastavitve [29].



Slika 3 Prikaz korakov dodeljevanja enoznačnih IP naslovov

3. Stikala in usmerjevalniki

3.1. Stikala (ang. Switch)

Omrežja so se sčasoma začela povečevati, z njimi pa se je povečeval tudi promet in število priklopljenih naprav. Zaradi povečevanja števila podatkov, s tem pa tudi prometa so stari razdelilniki (ang. HUB) postajali vse bolj neuporabni. Tako so razdelilnike zamenjala stikala.

Stikala so naprave, priključene v omrežja, ki posredujejo in filtrirajo pakete med priključenimi segmenti. Za razliko od razdelilnika, ki so prejete okvirje vedno pošiljali na vsa vrata, stikalo posreduje pakete na točno določena vrata. Delujejo na nivoju 1, 2 in 3 po ISO OSI modelu, pri čemer izvajajo samostojno učenje. Imajo več vrat, vsaka izmed njih pa v pomnilniku hrani naslovno tabelo[2]. Prednosti stikal so zmanjševanje števila posredovanj na vse naslove, omogočajo ločevanje omrežja [13].

Danes že vsa stikala omogočajo izvajanje dvosmernega prometa (ang. full-duplex option). Uporaba dvosmerne opcije izmenjave podatkov spremeni komunikacijska pravila tako, da lahko sprejema različne podatke, ki jih trenutno oddaja, pri čemer mora imeti vsaka naprava, ki je vpletena v komunikacijo, dostop do para fizičnega ožičenja [2].

Naslovna tabela hrani podatke o MAC naslovih – ciljni MAC naslov okvirja, vratih – vrata, ki morajo biti uporabljena za posredovanje okvirja za določen MAC naslov in Timer – ki služi kot identifikator starosti zapisa [12].

V primeru, ko stikalo prejme okvir, ki je namenjen prejemniku na istih vratih, stikalo tak paket zavrže. Ko stikalo prejme okvir, prebere njegov ciljni naslov, ga primerja z vrednostmi v naslovni tabeli in posreduje na ustrezna vrata. V primeru, da v naslovni tabeli še ne obstaja ciljni naslov, stikalo posreduje okvir na vsa vrata (ang. Broadcast).

3.2. Usmerjevalnik (ang. Router)

Za razliko od stikal usmerjevalniki, ki v lokalnem omrežju povezujejo med seboj naprave (računalnike, stikala, tiskalnike), usmerjajo okvirje, usmerjevalniki pa usmerjajo in posredujejo pakete [11].

Naloga usmerjevalnikov je usmerjanje in posredovanje paketov od znanih ali neznanih usmerjevalnikov na svetu, ti usmerjevalniki pa tvorijo jedro omrežja. Usmerjevalnik izvaja posredovanje tako, da na podlagi podatkov iz datagrama na omrežni plasti posreduje pakete iz vhodnega vmesnika na izhodni vmesnik znotraj usmerjevalnika [11].

Kako usmerjevalnik na logičnem omrežnem nivoju ugotovi, kateri so ostali logični segmenti v omrežju? To lahko usmerjevalnik prebere iz usmerjevalne tabele, ki je bila ročno pripravljena ali pa se je usmerjevalnik dinamično naučil od drugih usmerjevalnikov v omrežju.

Usmerjevalno tabelo si lahko predstavljamo izredno preprosto:

192.168.2.0/24 skozi 192.168.10.254

192.168.3.0/24 skozi 192.168.10.254

0.0.0.0/0 skozi 192.168.5.5

Pri prvih dveh zapisih bo usmerjevalnik pakete, ki so namenjeni na 192.168.2.0/24 in 192.168.3.0/24, posredoval na 192.168.10.254. Pri zadnjem zapisu pa bo usmerjevalnik vse pakete, za katere ne najde zapisa v usmerjevalni tabeli, posredoval na 192.168.5.5 [2].

Razlika med usmerjevalnikom in stikalom [2]:

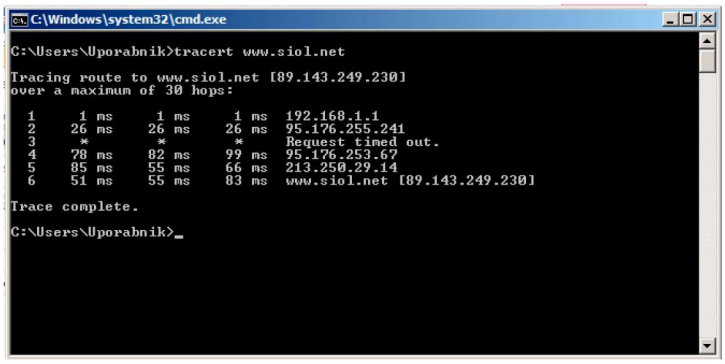
Stikalo	Usmerjevalnik
Uporablja iste omrežne naslove za vsa vrata	Uporablja različne omrežne naslove za vsa vrata
Tabela hrani MAC naslove	Tabela hrani omrežne IP naslove
Posreduje promet na vse vmesnike	Zavrača promet na vse vmesnike
Posreduje promet na neznane naslove	Zavrača promet na neznane naslove
Ne spreminja okvirjev	Izdela novo glavo
Lahko posreduje promet glede na okvirju glave (ang. frame header)	Promet se razvrsti v vrsto (FIFO) preden je posredovan naprej

3.3. Usmerjanje

Paketi za potovanje po omrežju potrebujejo navodila, kam morajo potovati, da dosežejo cilj. Prehajanju paketov po omrežju rečemo usmerjanje, to je mehanizem izbiranja poti pri prehodu podatka skozi omrežje. Usmerjanje bi si lahko predstavljali tudi kot potovanje iz Ljubljane do Maribora, pri čemer bi na vsakem križišču vprašali neznanca za smer in si smer zabeležili na papir.

Ker pa omrežje povezuje na milijarde omrežnih usmerjevalnikov, ima paket skoraj na vsakem vozlišču več možnih poti, vedno pa mora izbrati najboljšo. Za izbiro (najboljše) poti skrbijo kompleksni algoritmi, ki nenehno preverjajo stanja naslednjih vozlič, njihove poti pa shranjujejo v usmerjevalne tabele.

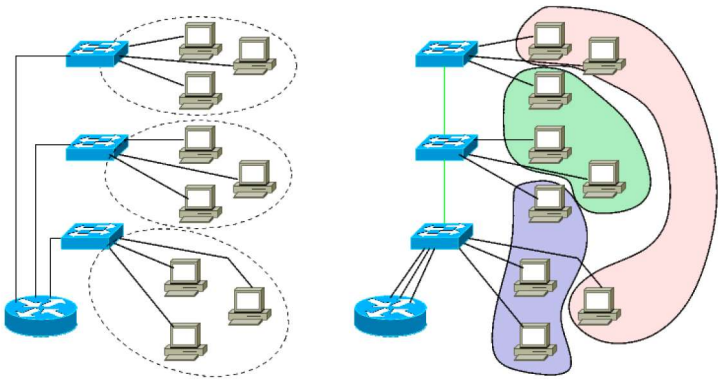
To omogoča usmerjevalniku, da v vsakem trenutku s pomočjo usmerjevalne tabele ve, kam mora usmeriti paket. Spodnja slika [Slika 4] prikazuje potek usmerjanja komunikacije od izvornega lokalnega omrežja do cilja naslova siol.net [8].



Slika 4 Prikaz poti med izvorom in ciljem(siol.net)

4. Ločevanje omrežja ali segmentacija omrežja

Pri večjih omrežjih klasična zgradba omrežja ne zagotavlja zadostne stopnje varnosti in zanesljivosti. Zaradi tega je prišlo do razvoja novih pristopov LAN in VLAN segmentacije. Segmentacija je deljenje omrežja na več manjših omrežij (podomrežja), pri tem pa vsako podomrežje tvori logično celoto. Z vpeljavo segmentov (podomrežij) omogoča zmanjševanje klicev na vsa vrata (ang. Brodcast storms), preobremenitve in možnost za zamašitve.



Slika 5 Prikaz klasične LAN segmentacije in VLAN segmentacije

4.1. LAN ločevanje

Ko govorim o LAN ločevanju ali segmentaciji, govorim o fizičnem ločevanju omrežja na podomrežja, kjer so posamezna manjša podomrežja fizično povezana na enoto (razdelilnik, stikalo, router), kot je prikazano na sliki [Slika 5] zgoraj levo.

Z ločevanjem omrežja na manjša podomrežja razširjamo omrežja, zmanjšujemo zamašitve in povečamo varnost. Ločevanje se izvaja v ISO OSI modelu na nivoju 2 [12].

4.2. VLAN – navidezna krajevna omrežja

VLAN ločevanje je tehnika ločevanja LAN omrežja na logične enote VLAN-e. To napravam omogoča, da niso več odvisne od geografske ali fizične lokacije [Slika 5]. Stikalo s pomočjo programske opreme določi, kateremu VLAN-u pripada okvir.

Za določanje VLAN pripadnosti stikala uporabljamo dve metodi. Prvo imenujemo eksplicitno označevanje, kjer stikalo sprejema podatke in jih označi z VLAN identifikatorjem, drugo pa implicitno označevanje, kjer ima stikalo pred nastavljena vrata, ki pripadajo določenem VLAN-u.

Promet lahko označujemo na več načinov:

- glede na vrata, na katera je prispel promet. Pri metodi določanja glede na vrata upravljavec predpripravi vrata na stikalu za posamezni VLAN. Ta pristop je najenostavnejši in najbolj razširjen. Slabost določanja VLAN-ov po metodi vrat je vnovična konfiguracija vrat pri menjavi naprave iz enih na druga vrata.

- glede na strojni naslov naprave (ang. MAC). Označevanje po metodi strojnega naslova je postopek dodeljevanja VLAN identifikatorja glede na strojni naslov naprave, ki jo ima vsaka komunikacijska naprava, priklopljena v komunikacijsko omrežje. Ta pristop omogoča menjavo vrat lokacij brez posega upravitelja, vendar pa se slabost kaže pri menjavi komunikacijske naprave ali prehodu med stikali.

5. Požarne pregrade / zid

Da lahko prikažem, kaj požarna pregrada omogoča in kako se upravlja, moram najprej predstaviti, kaj požarna pregrada sploh je, čemu služi in kje se nahaja. Ideja zidu je zaščita območja pred vsiljivci. Podoben primer lahko najdemo pred več kot dva tisoč leti, ko je Kitajska zgradila kitajski zid, s katerim se je zaščitila pred vsiljivci, s tem pa občutno zmanjšala svojo ranljivost [5].

V poznih 80. letih prejšnjega stoletja je bila glavna naloga t.i. požarnih pregrad ločevanje omrežij med seboj. To sicer velja tudi danes, so pa v tem času »pridobile« tudi nove namene (funkcionalnosti). Požarna pregrada, ki jo mnogi imenujejo tudi robna požarna pregrada, je lahko namenska programska rešitev ali namenska naprava, torej skupek več naprav, katerih osnovna naloga je varovanje omrežij pred zunanjimi vplivi. Požarne pregrade najdejo svoje mesto na »robu« lokalnega omrežja, kjer paketi »varno« zapuščajo lokalno omrežje. Požarna pregrada s pomočjo varnostnih pravil varuje omrežje, v katero je vpeta [5,6].

Od pojava prve požarne pregrade do danes se je na tržišču zvrstilo več požarnih pregrad. Trenutno je dostopna četrta generacija oziroma Next generation firewall (ang.), krajše NGF.

Namen prve generacije požarnih naprav je bilo ločevanje ali paketno filtriranje (ang. packet filtering). To je pomenilo, da je požarna pregrada (glede na varnostna pravila) pakete sprejela ali zavrgla izključno na podlagi izvornega, ciljnega naslova in vratih [14,15].

Pri drugi generaciji požarnih pregrad so vpeljali nove mehanizme pregledovanja, tako imenovani povezovalni paketni pregled ali krajše SPI (ang. Stateful Packet Inspection). Požarna pregrada s tem ni več le ločevala pakete glede na izvorna ali ciljna vrata in naslov, temveč je s pomočjo mehanizma, imenovanega SPI, spremljala podatke od vzpostavitve seje pa vse do konca seje. Pri prehodu podatkov si požarna pregrada beleži stanja in ob prihodu novega paketa s pomočjo mehanizmov primerja novo stanje glede na obstoječo tabelo stanj ali je podatek del vzpostavljene povezave ali gre za ponovno vzpostavitev povezave, ki je v preteklosti že bila vzpostavljena in je bila prebrana v tabele stanj ali pa gre za novo sejo [14,15].

Tretja generacija požarnih pregrad je prinesla nov pristop nadzora, pristop s tako imenovanim aplikacijskim posredovanjem (ang. Application proxy). Identificirala je lahko nekaj ključnih storitev, protokolov, kot so na primer FTP (ang. File transfer protocol), DNS (ang. Domain Name System) in HTTP (ang. Hypertext Transfer Protocol). Požarne pregrade te generacije se obnašajo kot posredniki med uporabnikom in strežnikom, saj je za vsako izmed strani

vzpostavila ločene seje, pri tem pa preverila promet za morebitne viruse, nevarno vsebino paketov, nezaželene spletne strani [14,15].

V zadnjo, četrto generacijo požarnih pregrad pa se uvrščajo tiste, katerih delovanje ni več omejeno samo na nivoju 2 in 3 po ISO OSI modelu, kot je bilo pri prejšnjih generacijah, ampak se lahko pregledovanje izvaja prav na vseh nivojih. S pomočjo mehanizmov lahko pregledujejo promet in med prehodom identificirajo aplikacije, zaznavajo zlonamerno kodo, pregledujejo podatke z protivirusnimi programi, prepoznajo uporabnika. Pri prehodu paketov skozi požarno pregrado požarni pregradi ni potrebno več rušiti povezave in ponovno vzpostavljati povezave za pregledovanje vsebine [14,15].

Poglavitni mehanizmi, da se požarna pregrada lahko uvrsti v četrto generacijo požarnih pregrad, so IPS (ang Intrusion prevention system), IDS (ang. Intrusion detection system), DPI (ang. Deep packet inspection), možnost identifikacije in kontrole aplikacije uporabnikov glede na ustrezna pravila.

Sistem za zaznavanje in preprečevanje vdorov (IDS in IPS)

IDS (ang. Intrusion Detection System) je samostojna naprava ali programska oprema, ki je priključena v omrežje, njena naloga pa temelji na zajemanju in analiziranju prometa v realnem času. Pri pregledovanju prometa IDS odkriva in obvešča o morebitnih znakih škodljivega prometa za omrežje.

V postopku odkrivanja škodljivega prometa IDS deluje na kopijah podatkov, pri čemer nekaj škodljivega prometa vstopi v omrežje preden ga IDS uspe identificirati.

Prav tako kot IDS je tudi IPS (ang. Intrusion Prevention System) lahko samostojna naprava ali programska oprema, priključena v omrežje. Imata enake naloge, razlika je le v tem, da IPS blokira vstop prometu paketom, ki so bili prepoznani za škodljive. IPS analizira promet od nivoja 2 pa vse do nivoja 7 po ISO OSI modelu.

Ko IPS prejme paket, ta ni posredovan naprej na izhodni vmesnik, dokler paket ni pregledan in označen za neškodljivega. V primeru, da je označen za škodljivega, IPS blokira promet in vse nadaljnje pakete iz tega naslova, pri tem pa mora skrbeti, da ostala komunikacija teče nemoteno [16, 18, 19].

Bolj napredni oziroma novejši IDS-ji in IPS-ji uporabljajo kombinacijo dveh ali več algoritmov za odkrivanje škodljivega prometa:

- vzorčno primerjanje (ang. pattern matching) – iskanje zaporednih byte-ov v paketih (vzorcev), ki jih primerja z lokalnim ali oblačnim skladiščem z že znanimi vzorci škodljivih paketov,
- primerjanje paketov v kontekstu (ang. statefull matching) – iskanje in primerjanje vseh paketov v povezavi, ne samo enega paketa,
- snort – odprtokodni sistem, ki nam omogoča lastno pripravo vzorca, na katerega bosta IDS in IPS reagirala,
- protokolno odstopanje (ang. protocol anomaly) – iskanje odstopanja od standardov, od komunikacijskih protokolov (RFC – Request For Comment),
- odstopanje od prometa (ang. traffic anomaly) – iskanje nenavadnega prometa v omrežju, recimo nenadno povečanje število UDP paketov, nenadno vzpostavljanje novih storitev ali protokolov in podobno,
- statistična odstopanja (ang. statistical anomaly) – iskanje s pomočjo statističnega ovrednotenja varnega prometa, pri katerem se statistična vrednost nenehno dopolnjuje in izračunava,
- odkrivanje vdorov skozi zadnja vrata (ang. backdoor detection) – iskanje odprtih vrat, ki čakajo, da ji napadalec izkoristi za napad [16, 18, 19].

5.1. Požarna pregrada Palo Alto

Za reševanje problema sem izbral požarno pregrado naslednje generacije Palo Alto model VM-300. Model VM- 300 je nameščen v navidezno okolje, ki ga lahko zaženemo samo z uporabo navideznih operacijskih sistemov VmWare ESXi in Citrix NetScaler.

Tehnične zmogljivosti požarne pregrade modela VM 300 so:

- 250.000 istočasno vzpostavljenih sej,
- 2.000 IPSec VPN tunelov,
- 500 SSL VPN uporabnikov,
- 40 varnostnih območij,
- 5.000 nastavljenih varnostnih pravil,
- 10.000 shranjenih naslovov naprav,
- 1G bps prepustnosti z omogočenim App-ID*,
- 600 Mbps prepustnosti z analiziranjem prometa za potencialne grožnje*,
- 250 Mbps IPSec VPN prepustnosti*,
- 8.000 na novo ustvarjenih sej na sekundo*.

Vse karakteristike označene z * so bile izmerjene s strani proizvajalca v idealnih pogojih, z uporabo PAN OS 6.0 in 4-jedrnega procesorja [28].

Pri zasnovi požarnih pregrad so pri Palo Altu stopili korak naprej in starim funkcionalnostim prejšnjih generacij dodali nekaj poglavitnih novosti, s tem pa naredili velik napredek v primerjavi s konkurenco. Poglaviten razlog za spremembo je bil, da starejši pristopi zaščite omrežja niso več zadostovali. Zaščita omrežja po načelu pregledovanja vrat in naslova pošiljatelja ali prejemnika je bila namreč že nekaj časa nezadovoljiva, s tem pa tudi nevarna.

Za lažjo predstavo o ranljivosti omrežja vzemimo za primer uporabo aplikacije TeamViewer. TeamViewer, ki se uporablja za oddaljen dostop do tretjih računalnikov, poleg tega pa omogoča tudi prenos podatkov med lokalnim in oddaljenim računalnikom. Aplikacija TeamViewer za svoje delovanje uporablja standardna vrata 80, te pa med drugim uporablja tudi naš brskalnik, ki ga uporabljamo za brskanje po spletu. Ob uporabi aplikacije Teamviwer bi starejše požarne pregrade brez težav posredovale in sprejemale promet misleč, da vsebino proizvaja spletni brskalnik, čeprav bi bil promet lahko škodljiv.

Ključne novosti, ki jih izvajajo požarne pregrade Palo Alto, so:

- Identifikacija aplikacij APP ID: mehanizem prepoznavanja aplikacij se izvaja takoj po vhodu prometa v požarno pregrado. Vsaka aplikacija ima svoj enoličen aplikacijski podpis (ang. application signatur), kar omogoča APP ID, da jo lahko identificira. Vsi podpisi, ki jih APP ID zmore identificirati, se nahajajo v lokalnem ali oblačnem skladišču. Požarna pregrada se samodejno posodablja, proizvajalec naprave pa skrbi za najnovejše posodobitve aplikacijskih podpisov. APP ID nam omogoča tudi izdelavo lastnega aplikacijskega podpisa. S pomočjo vseh aplikacijskih podpisov naprava lahko identificira aplikacijo in skladno z varnostnimi pravili posreduje oziroma zavrne promet [8].

- Identifikacija uporabnikov USER ID: kot že samo ime pove, požarna pregrada poizkuša identificirati uporabnike, ki ustvarjajo promet. Uporabnika identificira s pomočjo povezave na različne uporabniške imenike (Microsoft Active Directory, Novel eDirecory, itd), terminalne storitve (Citrix, Microsoft terminal service), s pregledovanjem sistemskih dnevniških zapisov ali kakšnim bolj kompleksnim mehanizmom[21]. Tako varnostna pravila in nastavitve niso več strogo vezane samo na IP naslov, ampak se jih lahko poveže tudi z uporabniki.

- Identifikacija vsebine CONTENT ID: pri Palu Altu so funkcionalnost IPS-ja poimenovali CONTENT ID. Poleg funkcionalnosti, ki jih ponuja IPS, CONTENT ID omogoča še pregledovanje prometa z antivirusnim programom in možnostjo nadziranja in filtriranja spletnih naslovov [21].

Požarno pregrado lahko upravljam na dva načina: z ukazno vrstico (ang. CLI ali command line interface) ali preko spletnega brskalnika. Privzeto ima požarna pregrada prednastavljene naslednje podatke:

- IP naslov na 192.168.1.1
- uporabniško ime in geslo na admin/admin.

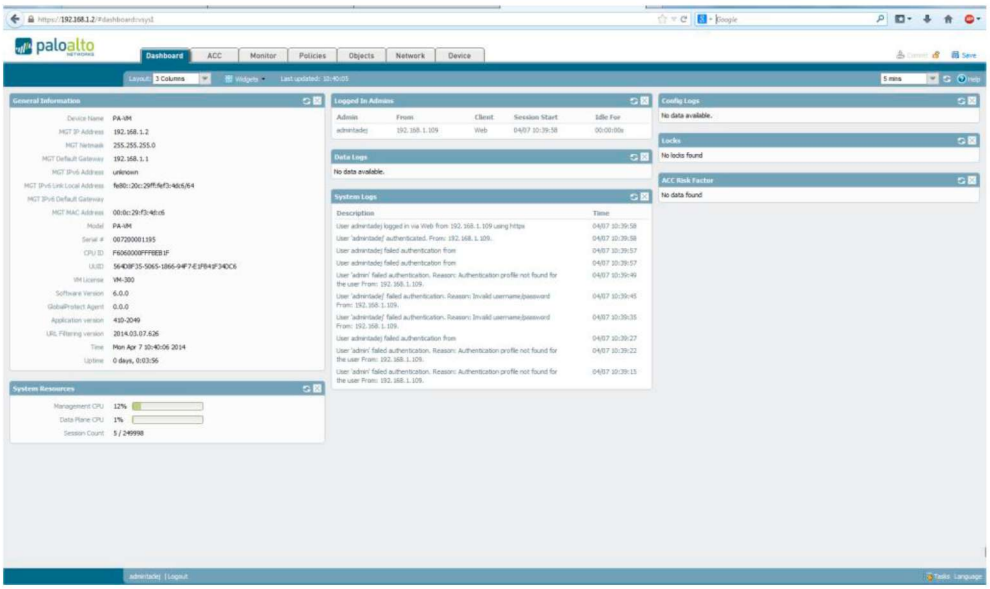
Privzeti naslov je nastavljen na posebnem vmesniku na požarni pregradi, ki je namenjen le upravljanju (ang. managment interface). To pomeni, da je promet, ki prihaja na upravljalni vmesnik, namenjen le upravljanju in ne splošni komunikaciji. Za prikaz delovanja dostopa preko ukazne vrstice bom uporabil program putty.exe, za dostop preko spletnega brskalnika pa enega od splošno znanih brskalnikov (Chrome, Mozilla itd.).

Zaradi lažjega upravljanja in ljudem bližjega grafičnega načina upravljanja bom večino korakov opravil z uporabo spletnega brskalnika.

Za dostop do požarne pregrade uporabim naslov upravljalnega vmesnika. Za prijavo - tako preko ukazne vrstice kot tudi spletnega brskalnika, uporabim uporabniško ime in geslo. Oba načina prijave privzeto uporabljata varno povezavo HTTPS in SSH.

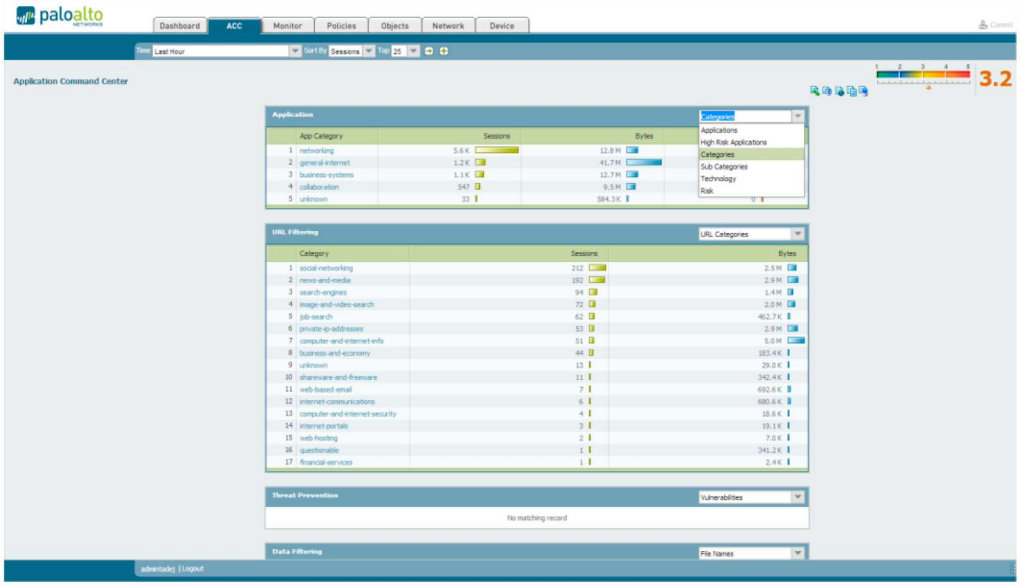
Grafični vmesnik je sistematično in čitljivo razdeljen na sedem sistematičnih sklopov (zavihkov):

- hiter pregled stanja požarne naprave (Dashboard): na enem mestu prikazuje splošno stanje požarne pregrade. Razdeljen je na več okenskih orodij (ang. widget), s katerimi si lahko po želji uredim videz. Namen pregledovalnika je hitrejše in učinkovitejše odkrivanje dvomljivega delovanja ali obnašanja (takoj po prijavi na požarno pregrado).



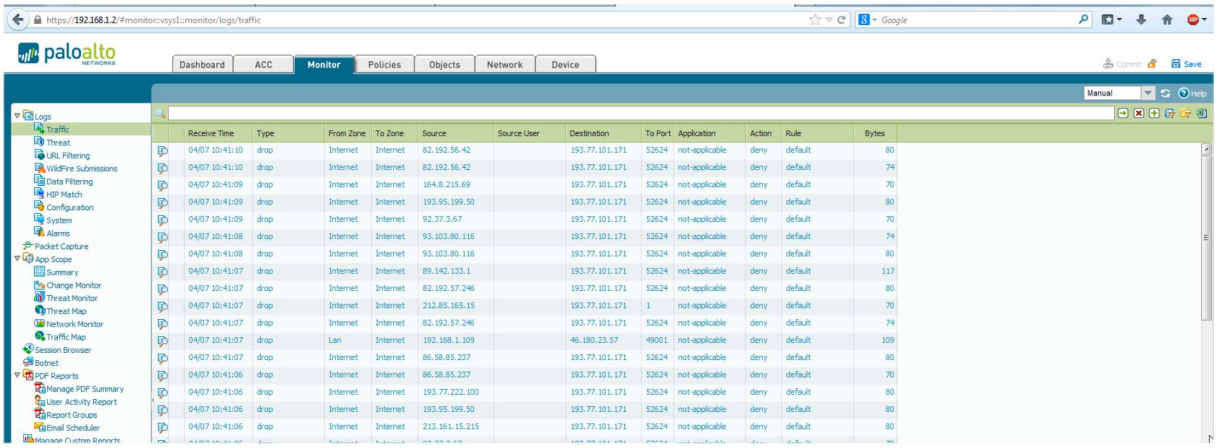
Slika 6 Prikaz izgleda osnovnega okna z najbolj pomembnimi podatki

- Analiza uporabe aplikacij (ACC ali Application command center) prikazuje trenutne aktivnosti, ki potujejo skozi požarno pregrado. Ukazni center je namenjen prikazovanju in analiziranju trenutnega stanja. Zaradi priročne grafične podobe lahko upravljalec hitreje in lažje odkrije potecialne grožnje. Vsak sklop (Application, URL Filtering, Data Filtering) se lahko razvrsti v podskupine, kot je prikazano na sliki [Slika 7] spodaj. Na sliki [Slika 7] je prikaz aplikacij, razvrščenih v kategorije, ki trenutno potujejo skozi požarno pregrado.



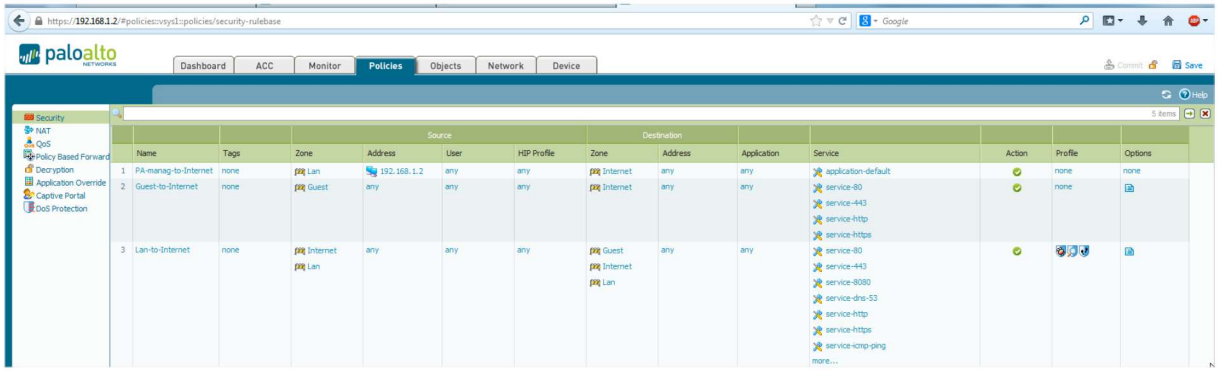
Slika 7 Prikaz ukaznega centra, ki prikazuje trenutne in pretekle aktivnosti zabeležene na napravi

- podrobnejši pregled zabeleženih dogodkov po posameznih kategorijah (Monitor) nam daje vpogled v dogodke, ki so že prispeli do požarne pregrade. Zabeleženi so vsi pomembni dogodki, ki jih upravljavec požarne pregrade potrebuje, vse od pregleda prometa (Monitor->Logs->Traffic), varnostnih dogodkov, IPS-ja, antivirusa (Monitor->Logs->Threat), pregleda dogodkov URL filtriranja (Monitor->Logs->URL filt.), pregleda DLP dogodkov in blokiranih datotek (Monitor->Logs->Data Filtering), sistemskih dogodkov (Monitor->Logs->System) pa vse do avtomatskega izdelovanja poročil o preteklem obnašanju naprave in preteklih dogodkih. Vse zabeležene dogodke je možno filtrirati po vseh stolpcih. Pri filtriranju si lahko pomagamo s posebnim namenskim grafičnim vmesnikom, s katerim lahko pripravim svoj filter.



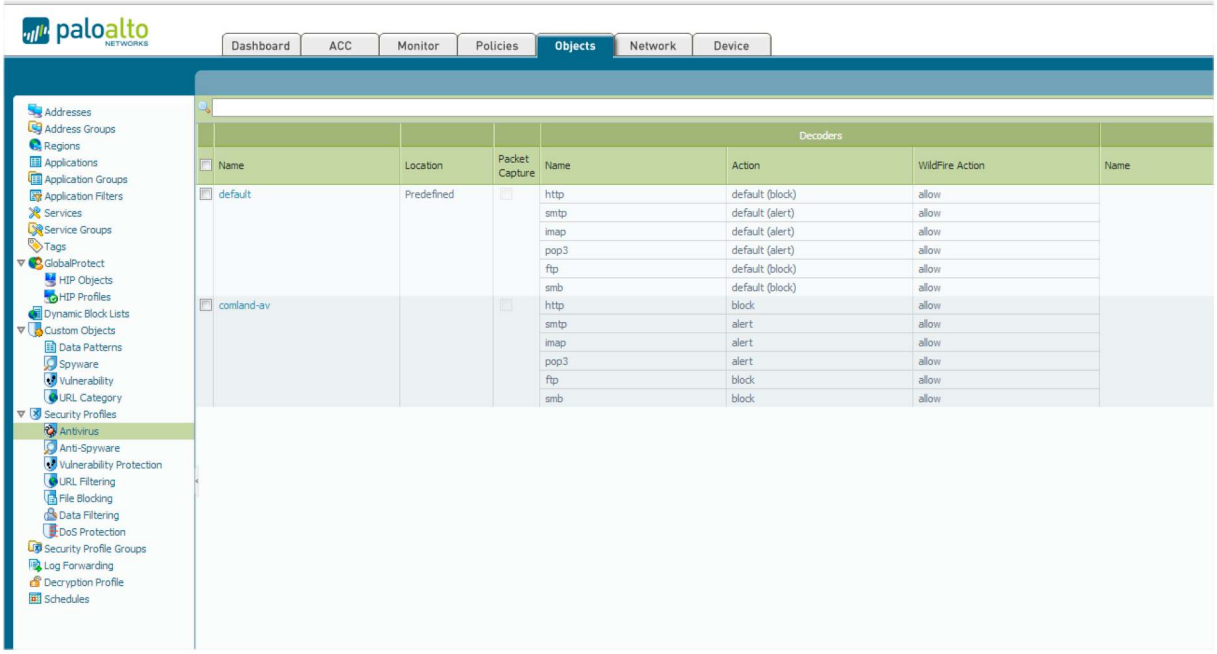
Slika 8 Prikaz izgleda zabeleženih dogodkov (prometa), ki so potovali skozi napravo

- Upravljanje z varnostnimi pravili (ang. Policies) – omenjeni zavihek nam daje vpogled in upravljanje z varnostnimi pravili, po katerih bo požarna pregrada dovoljevala oziroma ukrepala glede na promet, ki potoval preko požarne pregrade.



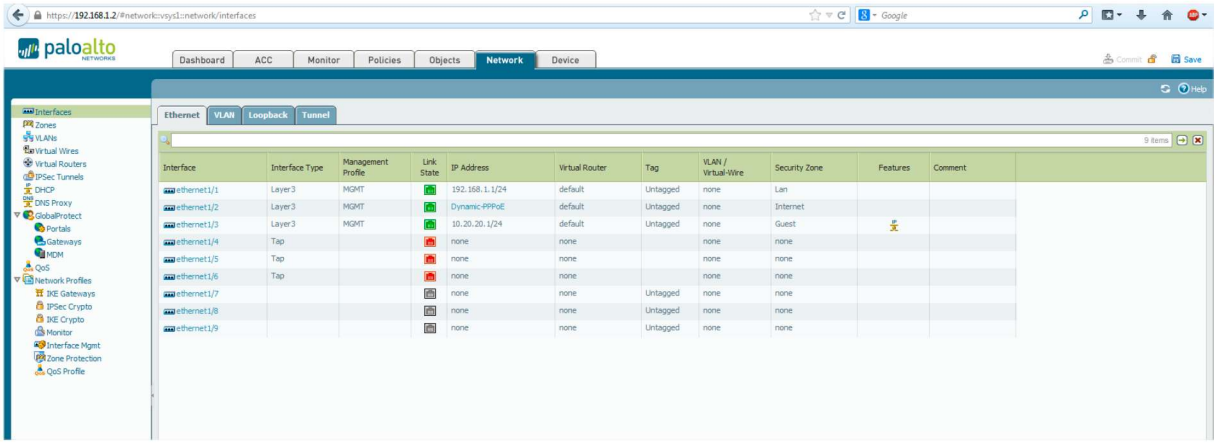
Slika 9 Prikaz izgleda zavihka za urejanje varnostnih pravil

- Objekti (ang. Objects) – ta sklop omogoča bolj sistematičen pristop za pripravo različnih poimenskih skupin, na primer IP naslovov, aplikacij, storitev, varnostnih profilov itd., ki jih pozneje lahko uporabim pri nastavitvi požarne naprave. S pomočjo tako sistematičnega pristopa poimenovanja je različnim upravljavcem požarne pregrade omogočeno lažje razumevanje in nastavljanje požarne pregrade.



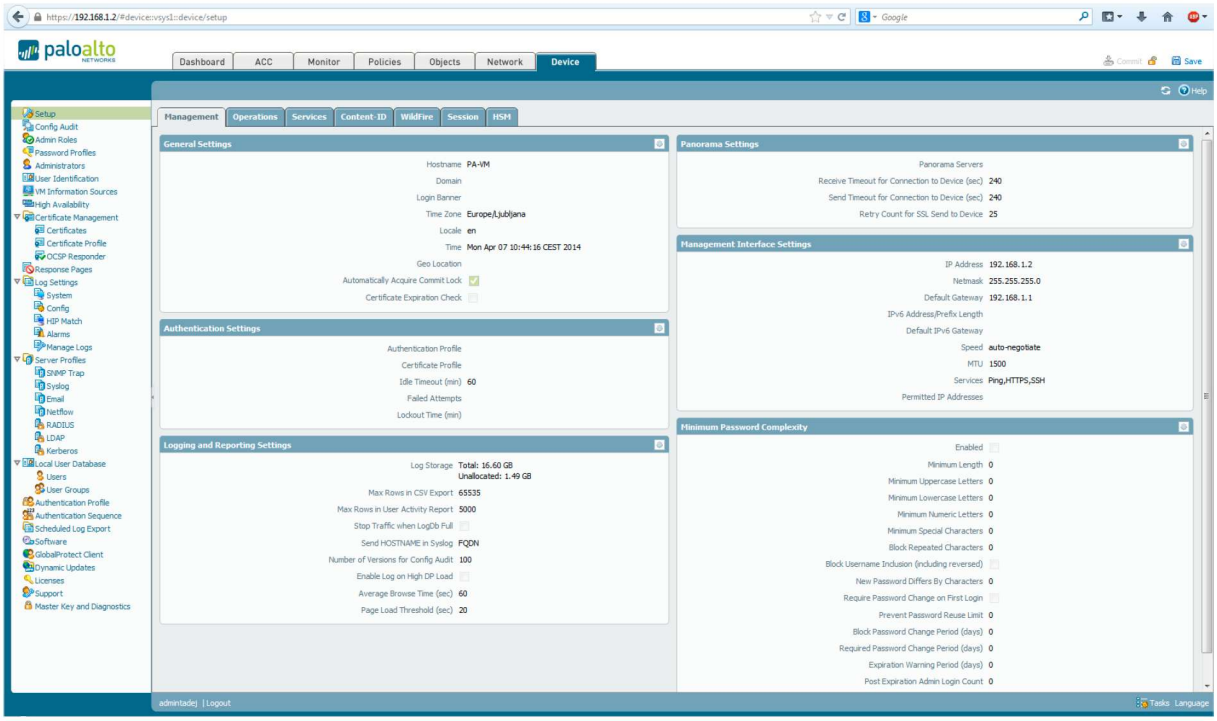
Slika 10 Prikaz zavihka za pripravo objektov

- Sklop mrežne nastavitve (Network): to je zavihek, ki je največkrat uporabljen pri prvi nastavitvi požarne pregrade in se pozneje, ko je naprava v delujočem produkcijskem okolju, ne spreminja več veliko. Ta zavihek je namenjen nastavitvam vmesnikov, varnostnih območij, virtualnih poti in virtualnih privatnih omrežij (pri Palo Altu so to funkcionalnost poimenovali Global protect).



Slika 11 Prikaz zavihka za nastavljanje vmesnikov

- Splošne nastavitve požarne pregrade (Device): zadnji zavihek je namenjen splošnim nastavitvam požarne pregrade. Tu se nastavlja uporabnike, ki lahko dostopajo do požarne pregrade ali uporabljajo Global protect, skupine uporabnikov, namenjen je spreminjanju privzetega upravljavskega naslova, nastavljanju posodobitev požarne pregrade in njenih posameznih funkcionalnosti, nastavitvi gesel, pregledovanju sistemskih dnevniških zapisov itd.

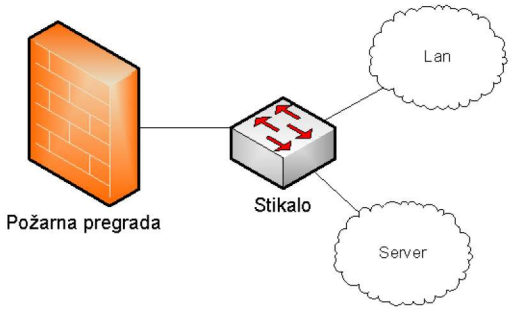


Slika 12 Prikaz zavihka za nastavljanje osnovnih nastavitev naprave

5.2. Vmesniki na požarni napravi

Kot sem v prejšnjih poglavjih omenil, vsaka naprava, ki komunicira v omrežju, mora imeti nastavljen vsaj en vmesnik. Izjema ni niti požarna pregrada. Na vsaki od požarnih pregrad Palo Alto je mogoče nastaviti vsaj osem vmesnikov, ki jih je možno nastavljati na različne načine. Ti načini so:

TAP – postavitev vmesnika v TAP način označujemo, ko vmesnik služi nadziranju prometa. Ta način se uporablja takrat, ko želimo pregledovati promet v omrežju, ki zaradi ločevanja omrežja ni direktno vpet na vmesnik požarne pregrade. Kot prikazuje slika [Slika 13], promet, ki poteka med strežniškim območjem prek stikala proti LAN območju, je zaradi ločevanja omrežja »neviden« za požarno pregrado. S postavitvijo vmesnika na požarni pregradi v TAP načinu in na stikalu omogočene funkcionalnosti SPAN, bi lahko požarna pregrada pregledovala promet, ki poteka med LAN in SERVER segmentom. SPAN funkcionalnost ali drugače rečeno SPAN vrata, je funkcionalnost CISCO stikal, ki prejete okvirje kopirajo in posredujejo na vrata, na katerih so omogočena SPAN vrata [1].



Slika 13 Prikaz postavitve požarne pregrade za TAP način

HA (ang. High Availability) ali visoka razpoložljivost – visoka razpoložljivost omogoča nemoteno delovanje sistema, za primere, ko zaradi človeških ali drugih dejavnikov pride do izpada delovanja požarne pregrade. Za postavitev požarne pregrade in delovanje visoke razpoložljivosti potrebujemo dve požarni pregradi, ki podpirata omenjeno funkcionalnost. Tako v primeru izpada delovanja ene požarne pregrade vlogo prevzame druga. V načinu visoke razpoložljivosti je vmesnik namenjen komunikaciji med dvema požarnima pregradama Palo Alto. Vmesnik na napravi služi le izmenjavi ključnih podatkov med požarnima pregradama, tako v primeru »okvare« delovanje prevzame druga [1].

Layer 2 – vmesnik v nivoju 2 v načinu po ISO OSI modelu povezuje naprave znotraj istega segmenta (VLAN-a/ov), pri čemer vmesnik nima IP naslova [1].

Layer 3 – vmesnik v nivoju 3 v načinu po ISO OSI modelu povezuje naprave iz različnih segmentov, pri čemer ima vmesnik določen IP naslov [1].

5.3. Varnostna območja

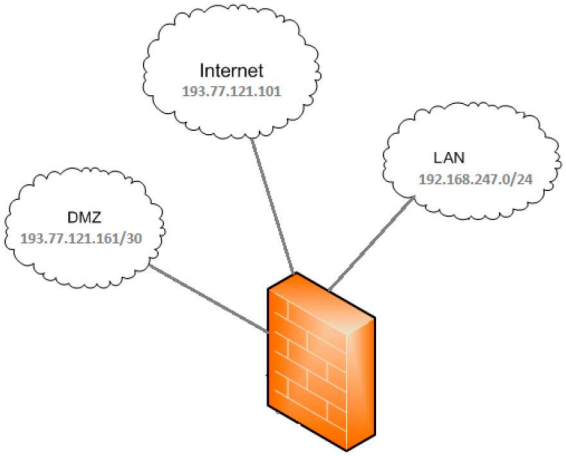
Požarne pregrade ločujejo omrežja v različne varnostne skupine. Vsako varnostno območje tvori ciljno skupino, ciljna skupina pa je lahko IP naslov, skupina naslovov, programski ali fizični vmesnik na požarni pregradi. Poimenovanje varnostnih območij mora biti čim bolj smiselno, razumljivo in je popolnoma prepuščeno upravljavcu. Največkrat uporabljen pristop poimenovanja je grupiranje po varnostnih skupinah, kot je prikazano na sliki [Slika 14].

Na njej so prikazana omrežne segmente, vpete na požarno pregrado. Razdeljena so na tri varnostna območja:

Internet – paketi, ki prihajajo iz interneta, so za lokalno omrežje, dokler niso popolnoma pregledani, najbolj tvegani. Zato so postavljeni v svojo varnostno skupino, ki se imenuje Internet.

Demilitarizirano območje (ang. DMZ ali Demilitarized Zone) je območje, kjer se največkrat nahajajo strežniki, ki morajo biti ves čas javno in lokalno dostopni. Med te uvrščamo poštne in HTTP strežnike. Na sliki [Slika 14] ga najdemo pod imenom DMZ.

LAN – privatno omrežje ali območje, kjer se nahajajo najbolj varne naprave. Na sliki [Slika 14] je označen z imenom LAN.



Slika 14 Prikaz segmentacije omrežja

Pri nastavitvi požarne pregrade ne smem spregledati potrjevanja kandidatov (ang. commit). Naprava nastavitvene spremembe, ki jih je izvedel upravljavec, shranjuje v ločeno nastavitveno datoteko, ki ji rečem kandidat za potrjevanje. Sprememba nastavitve požarne

pregrade ne učinkuje, vse dokler ji eksplicitno ne ukažem, naj sprejme trenutnega kandidata za delovno nastavitev. Ta postopek se izvede z ukazom ali klikom na gumb commit. Commit prepisuje trenutno delujočo nastavitev naprave s kandidatom za nastavitev.

5.3.1. 1. naloga: priprava topologije omrežja majhnega podjetja

Pripravi topologijo omrežja majhnega podjetja. Podjetje dela z večjim številom zunanjih strank, ki so za omrežje tvegana. Podjetje ima pa tudi lastne zaposlene. V svetovni splet se povezujejo preko ADSL povezave. Omrežje smiselno loči na tri podomrežja. V shemo umesti še požarno pregrado in jo dopolni tako, da omrežja, ki se vklapljajo na požarno pregrado, smiselno poimenuješ z imeni gost (ang. Guest), lokalno omrežje (ang. Lan) in internet (ang. Internet). Imena bodo pozneje uporabljena za pripravo varnostnih območij.

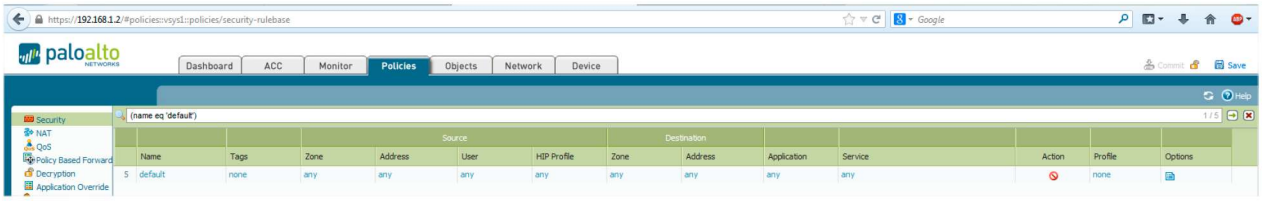
5.3.2. 2. naloga: priprava osnovni nastavitev za dostop in konfiguracijo požarne pregrade

Na požarni pregradi spremeni privzeti IP naslov upravljalnega vmesnika (managment interface) in:

a) Za vse tri segmente (gost, lokalno omrežje, internet) pripravi varnostna območja.
b) Za segment gost pripravi avtomatsko dodeljevanje enoznačnih IP naslovov v območju med 10.20.20.100 in 10.20.20.200. Pri tem si pomagaj s privzetim prehodom 10.20.20.1, primarnim (193.189.177.55) in sekundarnim (193.189.160.23) DNS-jem. Vmesnik Ethernet1/1 naj se odziva na naslov 192.168.1.1 z masko 255.255.255.0 (je del varnostnega območja lokalnega omrežja). Vmesnik ethernet1/2 naj bo nastavljen za vzpostavitev povezave PPPoE (je del varnostnega območja internet), na vmesnik ethernet1/3 pa nastavi tako, da bo poslušal na naslovu 10.20.20.1 z masko podomrežja 255.255.255.0 (je del varnostnega območja gost). Ne pozabi, da mora vsak vmesnik imeti usmerjevalno tabelo.

6. Varnostna pravila

V vsakdanjem življenju se srečujemo z okolji, kjer veljajo posebna pravila, ki jih je predpisala stroka ali pa kdo drug. Če se odpravljamo na potovanje z letalom, moramo upoštevati določena varnostna pravila, kot so prepoved nošenja nožev oziroma ostrih predmetov, orožja, tekočih snovi, katerih količina presega 25 mililitrov in drugo. Posebna varnostna pravila pa veljajo tudi na požarnih pregradah, ki jih določi upravljavec požarne pregrade, skladno z zahtevami za varno poslovanje in delovanje.



Slika 15 Prikaz pripravljenega varnostnega pravila

Pri požarni pregradi Palo Alto se za pripravo varnostnih pravil uporabljata dva načina. Pri prvem načinu želimo privzeto zavračati vso komunikacijo, ki prispe na požarno pregrado in z vsakim na novo dodanim pravilom omogočamo komunikacijo.

Drugi način pa je, ko privzeto dovolimo vso komunikacijo, z dodajanjem pravil pa jo omejujemo. Izbira načina priprave varnostnih pravil je prepuščena upravljavcu požarne pregrade, vendar ni odveč omeniti, da mu lahko napačna izbira pristopa povzroči resne težave pri poznejšem upravljanju. Če bo omrežje, ki ga bo ščitila požarna pregrada, bolj zaprto, torej bo zanj veljal visok nivo restrikcije, je boljša izbira privzetega zavračanja komunikacije, v primeru bolj odprtega pa obratno.

Pri kreiranju pravil je potrebno upoštevati, da bolj, kot je pravilo splošno, nižje v seznamu je uvrščeno in obratno. Vsaka požarna pregrada ima vsaj eno ali več varnostnih pravil. Pri Palo Altu se ujemanje nastavljenih pravil izvaja od prvo pripravljenega varnostnega pravila do zadnjega, kot si sledijo nastavljene v vrsticah ena za drugo. Pri tem pa je vedno zadnje pravilo privzeto pravilo.

Vsem pripravljenim varnostnim pravilom lahko ročno zamenjamo vrstni red v seznamu. Ko požarna pregrada prejme paket, preveri ujemanje s prvim pravilom v seznamu varnostnih pravil. V primeru neujemanja nadaljuje s primerjanjem z drugim pravilom v seznamu varnostnih pravil, ta postopek ponavlja vse dokler ne pride do ujemanja.

V primeru, ko se ujemanje ne ujema z nobenim pravilom, se izvede privzeto pravilo (ang. default policies). Pri pripravi pravila se preverja oziroma nastavljajo naslednje nastavitve:

Izvorno/i:

varnostno območje (ang. Zone) – izvorno varnostno/a območje/a, od koder bo prihajal promet

naslov (ang. Address) – izvorni naslov/i, od koder bo prihajal promet

uporabnik (ang. User) – izvorni uporabnik/i, ki bo oziroma bodo pobudnik/i ustvarjanja prometa

stanje naprave (HIP Profile) – izvorno stanje pobudnika/ov naprave

Ciljno/i:

varnostno območje (ang. Zone) – izvorno varnostno/a območje/a, od koder odhaja promet

naslov (ang. Address) – izvorni naslov/i, od koder bo šel promet

Aplikacija (ang. Application) – aplikacije, na katere bo pravilo vplivalo

Storitev (ang. Service) – naslovi vrat (ang. Port) in storitev

Kategorizacija naslova (ang. URL category) – kategorizacija vsebine naslovov

Končne akcije – ali se promet sprejme ali zavrže, kje se zabeleži promet v beležko dogodkov, omogočanje pregledovanja prometa z antivirusnim programom, zlonamerno kodo, … [2]

6.1.1. 3. naloga: priprava varnostnih pravil

Pripravi varnostna pravila, ki bodo dovoljevala promet iz varnostnega območja: lokalno omrežje proti gostu, lokalno omrežje proti internetu, gost proti internetu, omogoči storitve HTTP (vrata 80), HTTPS (vrata 443), med vsemi varnostnimi območji dovoli aplikacijo Ping, razen iz območja gost proti lokalnemu omrežju. Preveri, katere nastavitve ne delujejo in zakaj.

7. Preslikovanje naslovov (NAT)

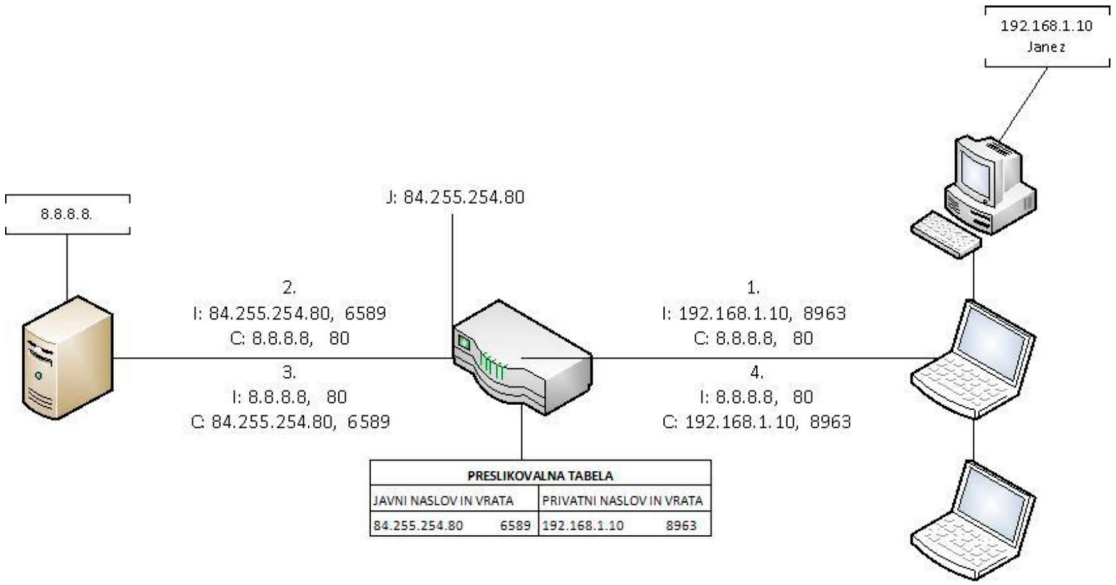
Kmalu po izumu interneta in po skokovitem vzponu uporabnikov oziroma naprav, ki uporabljajo javne enoznačne naslove za komunikacijo s svetovnim spletom, se je izkazalo, da bo mejna številka 4.294.967.296 naslovov kmalu presežena. Zato smo začeli naprave združevati v manjša zasebna omrežja (t.i lokalna omrežja), ki uporabljajo enega ali več javnih naslovov, ki so nam bili dodeljeni s strani ponudnika internetnih storitev.

Po standardih Internet Assigned Number Authority (IANA) RFC 1918 je vsaki napravi v lokalnem omrežju lahko dodeljen naslov iz naslovnega prostora: med 10.0.0.0 in 10.255.255.255, med 172.16.0.0 in 172.31.255.255 ali med 192.168.0.0 in 192.168.255.255. Ti se lahko ponavljajo v različnih lokalnih omrežjih, pri čemer ti naslovi ne nastopajo v svetovnem spletu. Ker so ti naslovi rezervirani za lokalna omrežja, paketi naj ne bi zapuščali lokalnega omrežja, v kolikor pa paket zaide v javno omrežje, ga prvi javni usmerjevalnik zavrže [22].

Da lahko paket zapusti lokalno omrežje, doseže cilj in se vrne nazaj v lokalno omrežje, se morajo naprave v lokalnem omrežju predstavljati kot ena naprava z enim javnim naslovom. Za to poskrbi tehnika preslikovanja naslovov (ang. NAT oziroma Network Address Translation) [23].

NAT je bil razvit predvsem zaradi pomanjkanja javnih enoznačnih naslovov. Omogoča nam, da lahko več naprav iz lokalnega omrežja komunicira s svetovni spletom ne glede na to, da imamo na voljo več naprav in le en javni naslov. NAT paketom s pomočjo mehanizmov na izhodu iz lokalnega omrežja zamenja zasebni naslov z javnim, pri tem pa v preslikovalno tabelo zabeleži izvorni in ciljni naslov ter vrata, da ve, kam mora posredovati vrnjeni paket [23].

V primeru komunikacije lokalnega omrežja s svetovnim spletom mehanizem preslikovanja NAT poteka v več korakih kot na sliki [Slika 16] :



Slika 16 Prikaz preslikovanja in komunikacije med odjemalcem in strežnikom

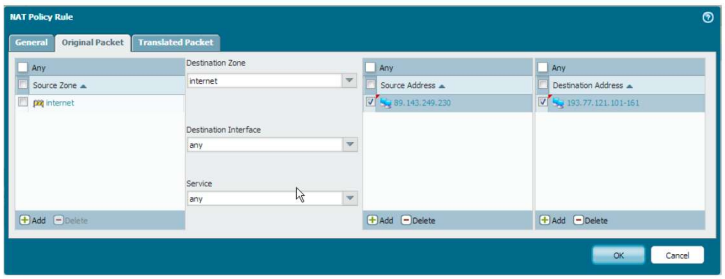
1.) Iz lokalnega omrežja uporabnik Janez na naslovu 192.168.1.10 začne s komunikacijo proti javnemu naslovu 8.8.8.8. Ko promet doseže usmerjevalnik, ta v usmerjevalno tabelo zabeleži izvorni privatni naslov in vrata, od koder je prišla komunikacija, v paketkih zamenja izvorni naslov z javnim naslovom usmerjevalnika in doda naključna vrata. Tako kot privatni naslov in vrata si v preslikovalno tabelo zabeleži tudi javni naslov in vrata.
2.) Usmerjevalnik posreduje preslikane pakete proti ciljnemu naslovu.
3.) Ciljna naprava odgovori na naslov, ki je bil zapisan kot izvorni naslov in vrata v prejetih paketih. Ko paket ponovno pride do usmerjevalnika, usmerjevalnik s pomočjo preslikovalne tabele zdaj točno ve, v kaj mora preslikati, da bo paket prišli nazaj do izvora.
4.) Usmerjevalnik preslika ciljni javni naslov 84.255.254.80 na vratih 6589 v 192.168.1.10 na vratih 8963, kot si je v prvem koraku zabeležil in posreduje pakete proti novemu cilju.

7.1. NAT preslikovanje na požarni pregradi PA

Vsi paketi, ki potujejo po omrežju, vsebujejo izvorni naslov, izvorna vrata, ciljni naslov in vrata, ki se nenehno spreminjajo. Pri Palo Alto so namestitvena okna, s katerimi nastavljamo preslikovalna pravila, razdelili v dva poglavitna zavihka, in sicer Original packet in Translated packet. Original packet je namenjen nastavitvam izvornih paketkov, preden jih mehanizem preslikovanja obdela.

Na tem zavihku se nastavlja, iz katerega varnostnega območja bodo prihajali paketi oziroma v katero ciljno varnostno območje so paketi namenjeni, na kateri vmesnik na napravi so namenjeni, katero storitev predstavljajo paketi, iz katerih izvornih naslovov prihajajo paketi in na katere ciljne naslove so paketi namenjeni.

Na primer: želim, da preslikovalno pravilo učinkuje na vse pakete, ki bodo prihajali iz izvornega naslova 89.143.249.230 na požarno pregrado (193.77.121.101), kot kaže slika [Slika 17].

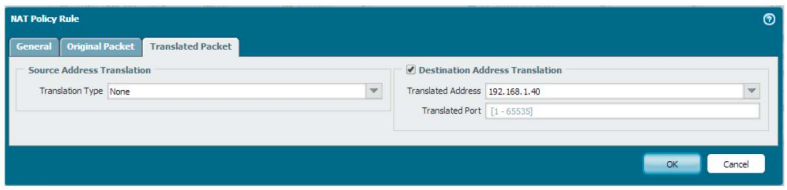


Slika 17 Prikaz pravila, ki bo učinkovalo na vse pakete, ki bodo prihajali iz določenega izvornega naslova na požarno pregrado

Translated packet je namenjen preslikovanju izvornih in ciljnih naslovov ali vrat paketom, ki so se v prejšnjem primeru ujemali s pravilom in na katere je preslikovalno pravilo učinkovalo. Pri pripravi pravila za preslikavo izvornega naslova lahko izbiram med:

- dinamičnim IP naslovom in vratom (ang. Dynamic IP And Port). Ta velja za največkrat uporabljeno preslikava, uporablja pa se takrat, ko želimo preslikati izvorni naslov paketa iz lokalnega omrežja v javni naslov, pri tem pa ne želimo ohraniti izvornega števila vrat.
- dinamičnim IP (ang. Dynamic IP), ki se uporablja, ko želimo, da se izvorni naslov paketa preslika v javni naslov, pri tem pa želimo ohraniti izvorno številko vrat. Ta nastavitev se med drugim uporablja, ko želimo, da je strežnik iz lokalnega omrežja javno dostopen na točno določenih vratih.
- statično opcijo (ang. Static). Ta se uporablja, ko imamo nek nabor IP naslovov A (192.168.1.0/24) in naslovov B (10.20.0.0/24) ter želimo, da se preslikava izvede iz točno določenega naslova iz množice A v točen določen naslov v množici B (192.168.1.1 v 10.20.0.1), pri tem pa ne želimo spreminjati vrat.

Pri preslikavah ciljnega naslova pa lahko nastavim le, v kaj se bo preslikal ciljni naslov, pri čemer lahko spremenim tudi vrata.



Slika 18 Prikaz preslikovalnega pravila za ciljni naslov. Pri preslikavi se bo zamenjal ciljni naslov originalnega paketa v ciljni naslov nastavljen 192.168.1.40

7.1.1. 4. naloga: priprava preslikovalnega pravila

Požarni pregradi pripravi preslikovalno pravilo, ki bo omogočalo komunikacijo naprav z internetom. Preslikovanje naj se izvaja na vseh lokalnih naslovih iz vseh varnostnih območij v naslov, ki je dodeljen napravi s strani ponudnika internetnih storitev.

8. Zaščita omrežja pred zunanjimi grožnjami, kot so virusi, zlonamerna koda, vdori

Prišel sem do točke, ko je požarna pregrada uspešno povezana s svetovnim spletom in z lokalnimi omrežji. Trenutne nastavitve požarne pregrade, ki sem jih podal v diplomski nalogi, predstavljajo delovanje starejših generacij požarnih pregrad.

Poglavitna prednost požarne pregrade Palo Alto v primerjavi s starejšimi požarnimi pregradami je, da je v enem samem prehodu prometa oziroma paketov skozi požarno pregrado sposobna preveriti morebitno škodljivost prometa za lokalno omrežje.

Obstajajo sicer rešitve, ki v prvem koraku sprejmejo pakete, ki jih nato posredujejo različnim namenskim napravam (IPS, IDS, AV), ki preverijo morebitno škodljivost podatkov za omrežje, pakete pa potem posredujejo naprej. Prav zaradi posredovanja paketov namenskim napravam (IPS, IDS, AV) se požarna pregrada Palo Alto od drugih rešitev razlikuje tudi v tem, da s tehniko enojnega prehoda (ang. Sigle Pass) preveri škodljivost paketov in s tem bistveno zmanjša zakasnitve v delovanju.

Omrežjem predstavlja grožnjo kakršnokoli spremenjeno delovanje ali obnašanje, ki bi vplivalo na tri poglavitna področja zaščite informacij:

- zaupnost: informacija mora biti na razpolago le tistim, ki so do nje upravičeni
- integriteta: informacijo lahko spreminja le tisti, ki je za to pooblaščen
- razpoložljivost: informacija mora biti vedno dostopna tistim, ki jo potrebujejo

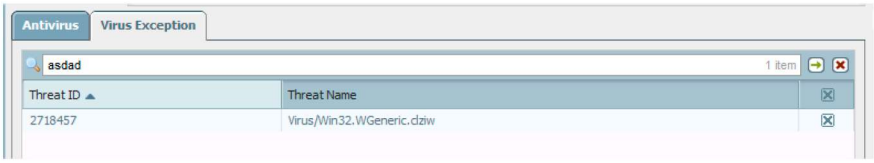
Požarna pregrada Palo Alto z vgrajenim mehanizmom za preprečevanje grožnje (ang. threat prevention) in enojnim prehodom podatkov skozi požarno pregrado skrbi za najnižjo možnost ranljivosti omrežja. Vsaka grožnja, ki jo požarna pregrada lahko identificira, je zapisana v lokalnem ali oblačnem skladišču. Ta skladišča groženj posodablja proizvajalec naprave [4].

Vsaka grožnja, ki jo požarna pregrada lahko identificira, ima določen enoličen identifikator (ang. ID), ime, kratek opis in nivo grožnje za omrežje (ang. Severity). Enolični identifikator in ime grožnje nam omogočata, da pri definiranju pravil bolj podrobno določimo, kaj bo naprava storila za določene vrste grožnje.

Slika 19 Prikaz dodatnih lastnosti groženj, ki jih požarna pregrada lahko identificira

Za zmanjševanje nivoja ranljivosti požarna pregrada Palo Alto uporablja:

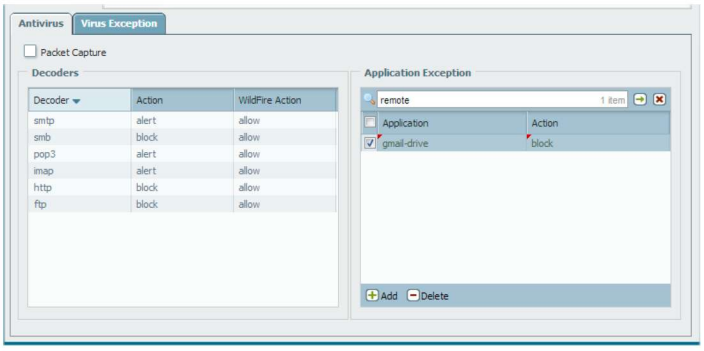
1. Antivirusni program: izraz virus, ki velja za enega najbolj poznanih izrazov, in sicer tako v naravi kot v računalniškem svetu, deluje po podobnem načelu. Virusi se širijo po principu zastrupljanja zdravih celic oziroma zdravih programskih datotek, z namenom uničenja ali onemogočanja delovanja. Antivirusni program s svojim delovanjem poizkuša predčasno preprečiti morebitne grožnje in težave, še preden virusi oziroma okuženi deli preidejo v delovanje. Naprava izvaja pregled prometa z antivirusnim programom na storitvah HTTP, FTP, SMTP, IMAP, POP3, SMB, pri čemer lahko za vsako akcijo nastavimo, kaj naj naprava naredi s prometom v primeru, če je odkrit okužen promet [Slika 20]. Akciji, ki jih lahko izvede, sta *blokiraj* (ang. Block), kar pomeni, da bo promet zavržen na vhodu, in ne bo posredovan naprej, in *obvesti* (ang. Alert), pri čemer naprava ne bo izvajala nobenih akcij nad prometom. V primeru okuženega prometa bo izvedla zapis v dnevnik (ang. Log), da je naprej posredovala okužen promet. Da bi se izognili morebitnim lažnim proženjem antivirusnega programa, nam omogoča nastavitev dveh izjem. Prva izjema, ki jo ponuja antivirusna zaščita, je nastavitev izjeme virusa (ang. Virus Exception), ki nam omogoča, da se antivirus ne bo prožil za virusne grožnje, katere smo dodali med izjeme. Izjema se uporablja, ko se antivirusni program odzove na promet, za katerega smo prepričani, da ni škodljiv. Na primer: na spletnem naslovu http://www.eicar.org/ se nahaja okužena datoteka, ki je namenjena testiranju antivirusnih programov. Ob prenosu datoteke bi antivirus sprožil alarm ali izvedel blokado prometa, čeprav vemo, da ta datoteka ni škodljiva. Če bi dodal med izjeme Threat ID: 1102199 Threat name: Virus/DOS.eicar-test-file.cd, se antivirus ne bi več prožil ob prenosu datoteke [7].



Slika 20 Prikaz dodajanja virusne izjeme

Druga izjema je *aplikacijska (ang. Application)*. Kot že samo ime pove, se aplikacijske izjeme nanašajo na izjeme, povezane z aplikacijami in so inicializatorke prometa. V primeru, da ne želimo, da antivirus preverja okuženost paketov, katere izvaja določen tip aplikacije, želeno aplikacijo dodam v aplikacijsko izjemo (ang. Application Exception). Za vsako aplikacijsko izjemo moram določiti tudi akcijo (ang. Action), ki naj jo antivirus izvede ob prepoznavi okuženega prometa. Akcije, ki jih lahko posamezne aplikacijske izjeme zavzamejo, so:

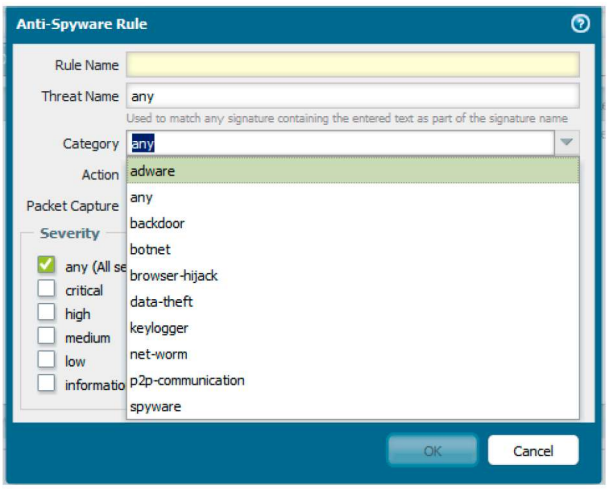
- dovoli (ang. allow), ne pregleduj prejetih paketov, ki jih je inicializirala določena aplikacija
- obvesti (ang. alert), v primeru okuženega prometa, ki ga je inicializirala določena aplikacija, shrani, obvesti z obvestilom in dovoli promet
- blokiraj (ang. block) in zavrzi ves okužen promet, ki ga je inicializirala določena aplikacija .



Slika 21 Prikazuje dodano aplikacijsko izjemo, ki bo zavrgla ves okužene pakete, ki ga bo nastal kot posledica Gmail Drivea.

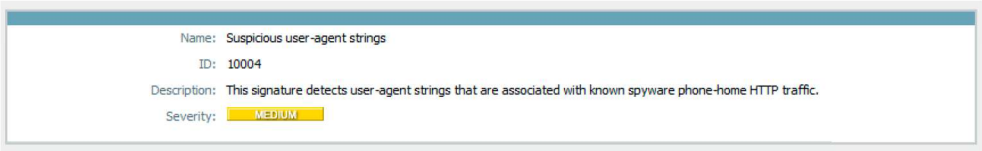
2. Program za odkrivanje vohunskih programov (ang. Anti SpyWare): vohunski program je tisti, ki se brez vednosti uporabnika namesti na računalnik, omogoča odtekanje informacij ali pa omogoča dostop do računalnika tretjim osebam. V preteklosti so se vohunski programi nahajali v priročnih programčkih, med nje uvrščamo ohranjevalnike zaslona (med tem ko se je program izvajal, je omogočal odtekanje informacij), danes pa se vohunski programi prenašajo ob obisku določenih spletnih strani brez vednosti uporabnika. Cilj vohunskih programov ni uničevanje programskih

datotek, temveč odtekanje informacij tretjim osebam. Informacije, ki jih le-ta koristi, so lahko zaupne narave. Med njih štejemo gesla, številke kreditnih kartic, e-mail naslove itd [18].



Slika 22 Prikaz kategorij vohunske programske oprema, ki jih lahko zazna naprava

Potencialne vohunske programe ali grožnje, ki jih je požarna pregrada sposobna identificirati, ima zapisane v lokalnem ali oblačnem skladišču, vsaka grožnja pa ima privzet nivo grožnje. Te nivoje določa proizvajalec požarne pregrade in jih nenehno posodablja, nivoji posameznih groženj pa lahko zavzemajo različne vrednosti: kritično (ang. critical), visoko (ang. high), srednjo (ang. medium), nizko (ang. low) ali opozorilno (ang. informational).



Slika 23 Prikaz privzetega nivoja varnosti in podrobnega opisa grožnje

Pravila za odkrivanje potencialnih groženj se lahko prilagajajo glede na tip *grožnje* (ang. Threat name), kar pomeni, da lahko navedemo točno grožnjo, za katero želimo izvesti točno določeno akcijo v primeru detekcije. Vsaka grožnja ima določen privzet *nivo grožnje*, kar pomeni, da se akcija ukrepanja ob odkriti grožnji primerja z nivojem (ang. Severity), nastavljenim v pravilu in prepoznanim privzetim nivojem grožnje, katerega je predpisal proizvajalec, ali *kategorijo* (ang. Category), ki predstavlja izvajane akcije glede na točno določeno skupino grožnje.

Akcije, ki se lahko izvajajo, ko požarna pregrada odkrije grožnjo, so: *blokiraj* (ang. Block), ki blokira ves okužen promet, *dovoli* (ang. Allow), ki dovoli okužen promet, *opozori* (ang. Alert), ki v dnevnik zapisov zabeleži okužen promet, požarna pregrada pa posreduje promet in *privzeto* (ang. default), ki izvede akcijo, predpostavljeno s strani proizvajalca požarne pregrade za tip prepoznane grožnje.

V zadnjem času se pojavljajo vohunski programi, ki spremljajo spletne strani, obiskane s strani uporabnika. Ne glede na to ali privzeta spletna stran, ki jo obiščete, že ima oglasna sporočila ali ne, se vam glede na zgodovino obiska oblikujejo reklamna sporočila, ki se avtomatično prikazujejo na vseh spletnih straneh v različnih oblikah.

3. Zaščita pred ranljivostjo (ang. Vulnerability Protection) - tako uporabniški računalniki kot strežniki za uspešno delovanje in opravljanje nalog potrebujejo namensko programsko opremo. Vsaka programska oprema ima poleg pozitivnih lastnosti tudi določene pomanjkljivosti. Te se izražajo ob slabše nastavljenih konfiguracijah programske opreme s strani uporabnika oziroma ob pomanjkljivo dodelani programski kodi. Slaba konfiguracija oziroma slabo programirana koda napadalcem lahko omogoča nepooblaščen dostop do računalnikov ali strežnikov. Za primer bi lahko navedel zadnjo znano grožnjo, imenovano Heartbleed, ki je zaradi nepazljivosti programerja programske opreme OpenSSL omogočala napadalcem dostop do gesel, ključev in občutljivih podatkov.

Slika 24 Prikaz dodane OpenSSL grožnje

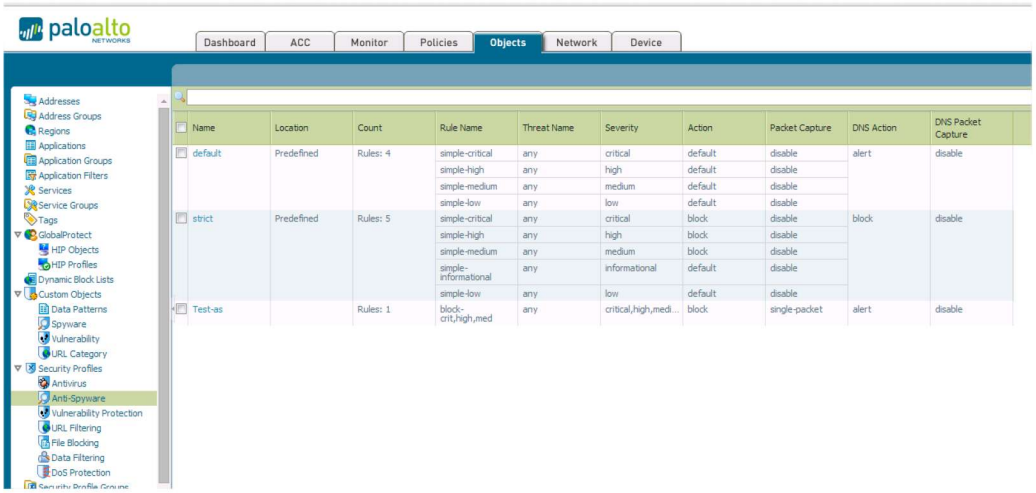
4. Filtriranje spletnih strani (ang. URL Filtering) – z mehanizmom prepoznavanja naslovov spletnih strani in s pomočjo lokalnega ali oblačnega skladišča podatkov o kategoriziranih spletnih straneh požarna pregrada razvršča spletne strani glede na kategorije: email, file-sharing, social-networing itd. Za podatke v lokalnih oziroma oblačnih skladiščih skrbi proizvajalec požarne pregrade, ki nenehno posodablja prepoznavne skupine. Če obiščemo spletne naslove facebook.com, twitter.com, linkedin.com, jih požarna pregrada prepozna kot kategorijo social networing, z enim samim pravilom pa lahko ukrepamo glede na kategorije teh strani.

Slika 25 Prikaz filtriranja URL kategorij

5. Data Blocking – odtekanje ali kraja inteligence je ena od mnogih groženj, ki pretijo organizacijam. Posredovanje informacij tretjim osebam lahko prinese nepopravljive posledice organizaciji. Da bi omilili takšne primere, si lahko pomagamo z mehanizmom blokiranja podatkov. Pri tem nam požarna pregrada omogoča spremljanje datotek, ki se prenašajo preko požarne pregrade v drugo omrežje. Omogoča nam tudi blokiranje odtekanja točno določenih tipov podatkov. Tako lahko poljubno blokiramo katerekoli tipe datotek.

6. Preprečevanje odpovedi storitev ali DOS napad (ang. DoS - Denial-of-service Protection) – napadalčev cilj je povzročiti odpoved storitve. Cilj takšne oblike napada je torej povzročiti okvaro sistema tako, da preobremenimo napravo (najpogosteje gre za strežnik), obremenitev pa se izvaja toliko časa, vse dokler ne odpovejo storitve, ki jih izvaja oziroma do odpovedi celotnega sistema. Najpogosteje se napad izvede tako, da napadalec pošlje strežniku zahtevek za vzpostavitev zveze z napačnim povratnim naslovom. Strežnik za vsak zahtevek locira del spominskega prostora, ki ga sprosti ob zaključku zveze. Ker pa strežnik odgovori na napačen povratni naslov, se zveza nikoli ne konča in spomin ostane zaseden. Tako napadalec z več zaporednimi ponovitvami prisili strežnik v pomanjkanje virov, kar privede do odpovedi storitev, preobremenitve, celo uničenja. Požarna pregrada s svojim mehanizmom prepozna tovrstne napade in zmanjša tveganje za omrežje.

Upravljanje z grožnjami, katere sem opisal zgoraj, se na požarni pregradi nahajajo na zavihku Object -> security profiles. Požarna pregrada ima že privzeta prednastavljena splošna pravila. Profilska zasnova upravljanja z grožnjami nam omogoča, da lahko pripravimo več različnih vrst varnostnih profilov, s katerimi bi kar najlažje zadovoljili varnost omrežja.



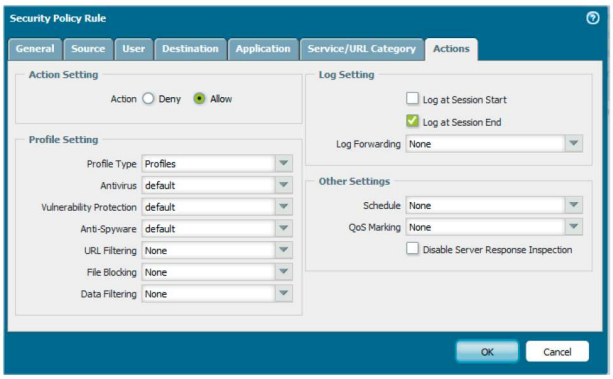
Slika 26 Prikaz različnih skupin profilov antispyware

Varnostne profile iz posameznih skupin lahko združujemo v globalne skupine (ang. Security profile Groups, zavihek Object -> Security profile Groups). Vsaka globalna skupina ima lahko nastavljen en profil iz vsake od skupin profilov, Antivirusa, AntiSpaywarea, Vulnerability Protectiona, URL filteringa, File blokinga, Data filteringa.

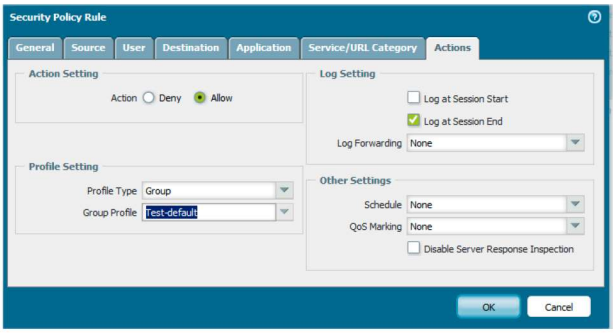
Preprost primer nastavitve globalnega varnostnega pravila je predstavljen na sliki [Slika 27], ki prikazuje globalno varnostno pravilo test-url, ki ima nastavljena varnostna pravila: antivirusni profil z imenom test-av, antispyware profil z imenom test-as, vulnerability protection z imenom test-ps in URL filtering z imenom test-url. Vsa našteta varnostna pravila na globalnem varnostnem pravilu so bila pred tem že nastavljena na zavihku Object -> Security profiles.

Slika 27 Prikaz nastavljenega globalnega varnostnega profila

Tako definirane globalne varnostne skupine profilov kot tudi posamezne skupine se po potrebi dodaja na posamezna varnostna pravila, ki veljajo za omejevanje ali dovoljevanje prometa na požarni pregradi. S takšnim pristopom lahko vsakemu pravilu nastavimo en globalni varnostni profil ali pa različna posamezna varnostna pravila.



Slika 28 Prikaz dodajanja varnostnih skupin na določeno varnostno pravilo



Slika 29 Prikaz dodanega globalnega varnostnega profila na določeno varnostno pravilo

8.1. 5. naloga: priprava pravila za preprečevanje ranljivega prometa

Obišči spletno stran (http://www.eicar.org/download/eicar.com) in si prenesi okuženo datoteko. Omenjena spletna stran omogoča simulacijo prenosa testnega primerka virusa, ki ne škoduje računalniku.

Ali naprava prepozna okuženo datoteko? Umesti anti spyware protection, anti-virus protection in Vulnerability Protection v najbolj smiselno varnostno pravilo, ki je namenjeno komuniciranju s svetom. Ponovno preveri na isti spletni strani, če po spremembi varnostni profili delujejo.

9. Upravljanje z aplikacijami

Poglavitna prednost požarnih pregrad naslednje generacije je prepoznavanje aplikacij. Poleg groženj, ki sem jih opisal v prejšnjem poglavju, za omrežje, organizacijo in združbe veliko nevarnost predstavljajo tudi aplikacije. Predvsem v poslovnem svetu se zaradi razlogov, kot so zmanjševanje delovne učinkovitosti, odtekanje dokumentov brez vednosti nadrejenih, nepooblaščeni vdori in podobno, velikokrat uporablja praksa dovoljenih oziroma prepovedanih aplikacij znotraj organizacije. Prestavljajmo si omrežje, ki ga ščiti požarna pregrada druge generacije. Požarna pregrada ima nastavljeno varnostno pravilo, ki dovoljuje promet na vratih 80. Vrata 80 namreč največkrat uporablja brskalnik za prikazovanje HTTP vsebine.

Za lažje razumevanje delovanja aplikacij, ki so lahko grožnja omrežju, si iz spleta prenesem program TeamViewer. TeamViewer je eden od mnogih programov, namenjenih oddaljenemu dostopu, ki omogoča dostop do računalnikov na oddaljenih lokacijah in pošiljanje ter prejemanja datoteke med računalniki.

TeamViwer nam omogoča, da na daljavo upravljamo oddaljeni računalnik, kot da bi fizično sedeli za računalnikom. Program privzeto deluje na vratih 80.

Ker oba programa, tako TeamViewer kot spletni brskalnik, delujeta na enakih vratih, čeprav opravljata čisto različne naloge, to predstavlja veliko grožnjo omrežju. Požarna pregrada bi v primeru uporabe TeamViwerja posredovala promet misleč, da na vratih 80 potuje promet, ki je bil inicializiran s strani spletnega brskalnika. Takšno vrsto komunikacije ne bi uspeli preprečiti s požarnimi pregradami brez prepoznavanja aplikacij.

Palo Alto za prepoznavanje uporablja mehanizem, imenovan AppID. AppID omogoča, da se takoj po vhodu paketov v požarno pregrado ugotovi obnašanje prometa. Prepoznavanje aplikacije poizkuša s štirimi mehanizmi:

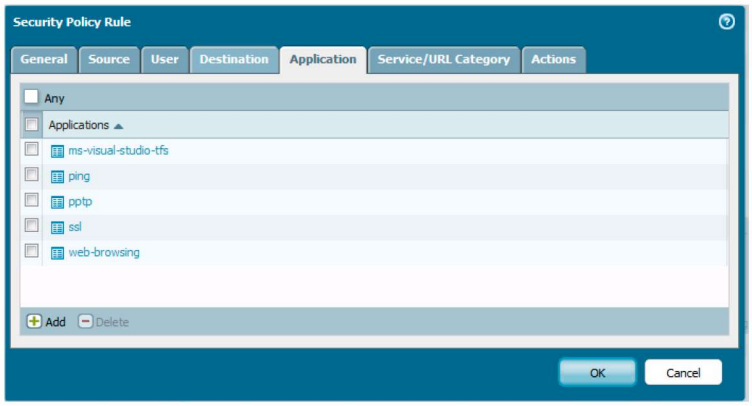
1. Preverjanje podpisov (ang. application signatures) - vsaka aplikacija med potovanjem po omrežju uporablja standardne lastnosti/obnašanje. To pomeni, da naprava ugotavlja ali aplikacija pri transportu uporablja standardna vrata protokola. Če naprava zazna promet, aplikacija za oddaljen dostop (RDP) preveri, ali uporablja njena standardna vrata 3389 ali katera koli druga. V primeru neujemanja, podatke za prepoznavanje posreduje naslednjim trem mehanizmom.
2. Dešifriranje SSL/SSH (ang. SSL and SSH Decryption) - promet, ki potuje po omrežju, je v veliki večini šifriran. Šifriranje prometa (o tem bom govoril v naslednjem poglavju) omogoča »skrivanje« vsebine pred nepooblaščenim vpogledom tretjih oseb, pri čemer inicializator in prejemnik komunikacije poznata pravo vsebino prometa.

Naprava prepozna, ali je prejet promet šifriran, v primeru šifriranega prometa ga dešifrira in posreduje nadaljnjim mehanizmom prepoznavanja.

3. Aplikacijsko in protokolno dekodiranje (ang. Application and Protocol Decoding) – s funkcijo dekodiranja požarna pregrada poizkuša odkriti dodatne lastnosti prometa, tudi tuneliranje aplikacij znotraj protokolov. Tuneliranje aplikacij znotraj protokolov je princip »skrivanja« prometa znotraj standardnega protokola. Za primer vzemimo že opisan primer (v poglavju Palo Alto) oddaljenega dostopa s programom TeamViewer, ko program uporablja standardni protokol HTTP, medtem ko se v resnici za njim skriva čisto drug promet.
4. Hervistična identifikacija (ang. Heuristics) - v primeru, ko nobena od zgoraj naštetih tehnik ni bila uspešna, naprava poizkusi prepoznati aplikacijo z metodo hervistične analize. Pri tem si pomaga s preverjanjem dolžine paketov, izvorom paketov prejetega prometa in že prepoznanih aplikacij. Preverja ujemanje [8].

Vse identificirane aplikacije, ki ji je naprava sposobna identificirati, se nahajajo v njenem lokalnem ali oblačnem skladišču in se dnevno posodabljajo in dopolnjujejo. Identificirane aplikacije lahko preverim na zavihku Object -> Application. Na seznamu identificiranih aplikacij se za vsako izmed aplikacij nahaja tudi podrobnejši opis, prikaz kategorije in podkategorije, v katero je razvrščena, številčno ovrednotena grožnja (ang. Risk) in katera vrata ter protokol uporabljajo.

Dovoljene ali zavrnjene aplikacije dodajamo na pripravljena varnostna pravila (zavihek Policies->Security). Vsako varnostno pravilo ima lahko vnesenih eno ali več aplikacij, ki jo bo varnostno pravilo dovoljevalo ali zavračalo.



Slika 30 Prikaz dodanih aplikacij na pravilo

9.1. 6. naloga: prepoznava aplikacije

Dopolni varnostna pravila tako, da:

- se iz varnostnega območja LAN proti gostu dovoli aplikacija MS-RDP. Preveri, ali se komunikacija vzpostavi. Poizkusi vzpostaviti povezavo z oddaljenim računalnikom na vratih 3388. Za vzpostavitev oddaljene povezave uporabi program Microsoft Terminal Services (start->mstsc.exe), za vzpostavitev povezave na drugih vratih pa z sintakso »IP naslov:3388«

- se iz varnostnega območja LAN proti Internetu onemogoči aplikacijo Gmail in preveri. V drugem koraku popravi varnostno pravilo in onemogoči samo Gmail-chat. Kaj se zgodi in zakaj?

10. Dešifriranje prometa

Da bi lahko razumeli, kaj dešifriranje prometa je, moramo najprej pojasniti, kaj je kriptologija. Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil ter razkrivanju podatkov. Njeni začetki segajo v čas rimskega cesarstva, natančneje v čas Julija Cezarja. Ker Julij Cezar ni zaupal svojemu dostavljavcu sporočil, je v celotnem sporočilu, katerega je dostavljavec prenašal, zamenjal črke za dve mesti. Tako je črka A postala D, B postala E in tako naprej vse do zadnje črke. Tako je lahko samo prejemnik, ki je vedel za zamik črk, vedel, kaj piše v sporočilu. Beseda kriptologija sicer izvira iz grščine: gre za skovanko besed kryptos, ki pomeni skrito in logos, beseda.

To je veda o tajnem komuniciranju, prisotna pa je na vseh področjih komuniciranja in shranjevanja pomembnih tajnih podatkov. Njen predmet proučevanja sta kriptografija in kriptoanaliza.

Kriptografija je veda, ki se ukvarja s tajnim pisanjem, njeni začetki pa najverjetneje sovpadajo z izumom pisave. Ukvarja se z razvojem metod in metodologij za šifriranje, z namenom dešifriranja šifriranega sporočila oziroma informacije. Njen namen je preprečevanje in odkrivanje zlorab. Ciljev kriptografije je več: ohranjevanje tajnosti pred nepooblaščenimi osebami, potrditev izvora informacije in identiteto ter zagotovitev, da informacija ni bila spremenjena [9].

S postopki dešifriranja šifriranih sporočil brez predhodnega poznavanja ključa pa se ukvarja kriptoanaliza. Ta se je razvijala istočasno s kriptografijo. Sestavljena je bila iz dveh grških besed: kryptos (skrito) in analyen (razrešiti).

Šifriranje in dešifriranje se izvajata po vnaprej določenem postopku, metodi ali algoritmu, pri katerem sporočilo z uporabo algoritmov spremenimo v šifrirano sporočilo. Postopek, po kakšnem principu pa je bilo sporočilo šifrirano, imenujemo ključ. Za uspešno šifriranje in dešifriranje sporočil morajo vsi vpleteni v komunikacijo poznati ključ, ki je bil uporabljen za šifriranje [21].

Poznamo dve splošni skupini šifriranja: simetrično in asimetrično.

Simetrično šifriranje je postopek, pri katerem se za šifriranje in dešifriranje uporabi isti ključ. Obe strani morata v tem primeru poznati šifrirni ključ. Prednost simetričnega šifriranja je preprostost ter hitrost šifriranja in dešifriranja. Največji problem in slabost je izmenjava ključev, še posebej, če je vpletenih več oseb. Vsaka mora imeti svojo kopijo ključa. Primer simetričnega šifriranja je način skrivanja informacij s strani Julija Cezarja.

Asimetrično šifriranje pa je postopek, kjer ima vsak vpleteni v komunikacijo po en zasebni in en javni ključ. Javni ključ je dostopen vsem, zasebnega pa pozna le lastnik ključa. Šifriranje poteka po naslednjem postopku: pošiljatelj šifrira sporočilo s prejemnikovim javnim ključem, prejemnik pa sporočilo, ki je bilo šifrirano s prejemnikovim javnim ključem, lahko dešifrira s prejemnikovim privatnim ključem. To pomeni, da se javni del ključa uporablja za šifriranje, zasebni del pa za dešifriranje. Asimetrično šifriranje je počasnejše od simetričnega, zato se ga v največji meri uporablja za izmenjavo ključa za nadaljnjo simetrično šifriranje.

10.1. SSL

Podatki se po spletu privzeto prenašajo v berljivi obliki. To tretjim osebam, ki uspejo prestreči komunikacijo, brez težav omogoča vpogled v vsebino paketa. S šifriranjem podatkov so podatki tistim, katerim podatki niso namenjeni, nerazumljivi, nerazumljivi so tudi tistim, ki jih lahko prestrežejo.

V ta namen so leta 1994 pri Netscape-u razvili SSL (ang. Secure Sockets Layer), varno komunikacijo med spletnim odjemalcem in strežnikom. Zaradi izredne uporabnosti in dobre implementacije je kmalu postal standard [22]. Pozneje so se razvili tudi naslednike, kot sta TLS (ang. Transport Layer Security) in WTLS (ang. Wireless Transport Layer Security).

SSL protokol z uporabo digitalnih potrdil zgradi varen tunel (ang. SSL tunel), ki skrbi, da je promet med dvema stranema šifriran, s tem pa neberljiv tretjim osebam. Digitalna potrdila so elektronske datoteke, ki izkazujejo identiteto ljudi, organizacij ali naprav. Zaupanja vredne digitalne certifikate izdaja certifikatna agencija (ang. Certificate Authorities (CAs)), ki poleg izdaje potrdil skrbi za njihovo pristnost. Digitalno potrdilo vsebuje privatni in javni ključ, ki se uporablja za šifriranje in dešifriranje podatkov. Javni ključ je namenjen šifriranju sporočil pošiljateljev in je lahko javno dostopen. Privatni ključ pa mora lastnik hraniti na varnem in izven dosega javnosti. Ko prejemnik sprejme pošiljateljevo šifrirano sporočilo, ga lahko dešifrira samo s svojim privatnim ključem. Dešifriranje je uspešno samo v primeru, ko je bila vsebina sporočila šifrirana s prejemnikovim javnim ključem [24,25].

SSL protokol je po ISO OSI modelu umeščen med transportni in aplikacijski nivo, skrbi pa za varno komunikacijo pri komunikaciji po internetu. Za svoje delovanje ima SSL privzeto rezervirane številke naslednjih aplikacijskih vrat.

Vrata	Protokol	Vrata	Protokol	Vrata	Protokol	Vrata	Protokol	Vrata	Protokol
443	HTTPS	465	sSMPT	563	NNTPS	614	SSL Shell	636	SSL-LDAP
989	FTP data	990	FTPS	992	Telnets	993	IMAPS	995	POP3S

Tabela 1 Šifrirni protokoli in vrata

Pri vzpostavljanju varne SSL komunikacije med strežnikom in odjemalcem SSL poskrbi za šifrirano izmenjavo sporočil. Algoritmi, ki jih lahko uporablja SSL protokol, niso fiksirani, določa jih lahko posameznik. Algoritmi, ki so trenutno na voljo, so: DES, 3DES, RC4, AES-CBC mode, AES-GCM mode, NGE1, AES-GCM, DH-768, RSA-768, DSA-768, DH-2048, RSA-2048, DSA-2048, DH-2048, RSA-2048, DSA-2048, MD5, SHA-1, SHA-256, SHA-384, SHA-512, HMAC-MD5, HMAC-SHA-1, ECDH-256, ECDSA-256, ECDH-384, ECDSA-384, ECDH-384, ECDSA-384 [26].

Šifrirne algoritme razvrščamo v štiri skupine:

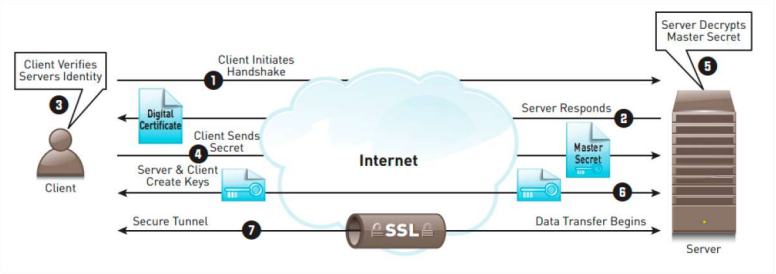
- Simetrične ključe (ang. Semmantic key): semantični algoritmi uporabljajo isti ključ za šifriranje in dešifriranje. DES, 3DES in RC4 se uvrščajo med simetrične algoritme, medtem ko se je potrebno AC4 in DEC algoritmoma izogibati zaradi majhnega ključa. Slednja nista več varna za uporabo. Pri uporabi algoritma AES je najmanjša priporočljiva dolžina ključa 256 bitov ali daljša [26].

- Javne ključe (ang. Public key): algoritmi z javnimi ključi uporabljajo različna ključa za šifriranje in dešifriranje, zasebnega in javnega. Zasebni ključ hrani lastnik ključa, javni del pa je na voljo tretjim osebam. V to skupijo spadajo RSA, RSA-768, DSA-768 in DH-2048 (Diffle-Hellman) [26].

- eliptične krivulje (ang. EEC ali Elliptic Curve Cryptography): princip delovanja EEC je pretvorba poljubnega sporočila omejene dolžine v celo število, v točki krivulje. V to skupino spadajo ECDH-256, ECDSA-256, ECDH-384, ECDSA-384, ECDH-384 in ECDSA-384. Ta način šifriranja počasi izpodriva šifrirne algoritme, ki temeljijo na faktorizaciji celih števil, kot sta npr. RSA in DSA [26].

- Zgoščevalni (ang. Hash) ali drugače rečeno zgoščevalni algoritmi, iz katerih je nemogoče v obratnem postopku izračunati fiksni del, iz katerega je bil izračunan rezultat zgoščevalnega algoritma. V to skupino spadajo Secure Hash Algoritem 1 (SHA-1), SHA-256, SHA-384, SHA-512, HMAC-MD5 in HMAC-SHA-1 [26].

Vzpostavitev varne komunikacije je razdeljena v dve glavni fazi: SSL rokovanje (ang. SSL handshake) in SSL izmenjava podatkov (ang SSL data transfare). V prvi fazi se izmenja ključ za šifriranje, v drugi fazi se začne varna povezava. Ti dve osnovni fazi sta poenostavljeno razdeljeni v 7 korakov:



Slika 31 Prikaz šifrirnega poteka med odjemalcem in strežnikom

Prvi korak:

Rokovanje se začne, ko odjemalec zahteva vzpostavitev varne povezave. Odjemalec posreduje seznam šifrirnih algoritmov in verzije algoritmov [25].

Drugi korak:

Prejemnik zahtevka za varno povezavo iz prejetega seznama izbere najmočnejši šifrirni algoritem in o izbiri obvesti pobudnika povezave. Prejemnik dodatno pobudniku posreduje digitalni certifikat, ki vsebuje ime strežnika, podatke izdajatelja digitalnega potrdila in javni ključ prejemnika zahtevka za vzpostavitev varne povezave. Prejemnik lahko v odgovoru zahteva, da se pobudnik vzpostavitve povezave predstavi z digitalnim potrdilom. Predstavitev pobudnika vzpostavitve povezave največkrat srečamo pri spletnem bančništvu, Fursu in še kje [25].

Tretji korak:

V tretjem koraku pobudnik preveri pristnost prejetega javnega ključa in preveri ali je izdajatelj javnega ključa zaupanja vredna agencija. Seznam zaupanja vrednih izdajateljev digitalni potrdil se največkrat hrani lokalno [25].

Četrti korak:

V kolikor je digitalno potrdilo veljavno, pobudnik izračuna osnovo za simetrični ključ, ga šifrira z javnim ključem prejemnika in posreduje prejemniku. Prejemnik sprejme šifriran ključ in ga dešifrira z zasebni ključem [25].

Peti korak:

Pobudnik in prejemnik si izmenjata glavna ključa, s katerim nadaljujeta simetrični princip šifriranja [25].

Šesti korak:

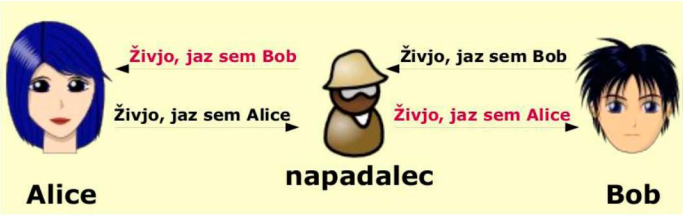
Zaključi se rokovanje in prenos podatkov po varni povezavi se začne. V kolikor katerikoli od zgornjih korakov spodleti, vzpostavitev varne povezave ne uspe [25].

10.2. Grožnje šifriranju

Z leti in napredkom tehnologije so se začele pojavljati ranljivosti in pomanjkljivosti šifrirnih mehanizmov. Da bi lahko dešifrirali komunikacijo, ki je šifrirana z 256 bitnim simetričnim algoritmom, bi v teoriji potrebovali $3 * 10^{51}$ let, kar je teoretično seveda nemogoče izvedljivo [25]. Z drugimi besedami povedano: če sem vlomilec in želim vlomiti v hišo, obstaja vsaj deset tisoč ključev vhodnih vrat, ki odklepajo vrata izbrane hiše.

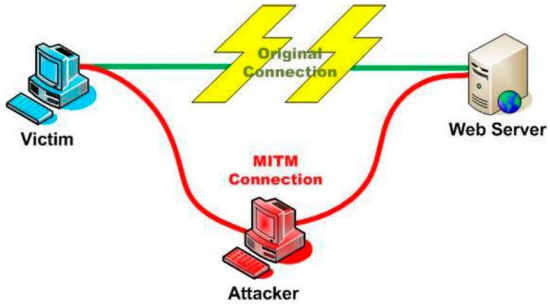
V tem primeru ne bom sedel pred vrati in preizkusil vseh deset tisoč ključev, ampak bom poizkušal priti v hišo na kakšen drugačen način - skozi okno, zadnja vrata, itd. Zakaj bi torej želel napasti šifrirni algoritem, namesto da bi napad izvedel v trenutku (pred začetkom) SSL rokovanja, ko povezava še ni šifrirana. Prav s takšnim pristopom razmišljanja so se napadalci lotili napadov na učinkovite šifrirane algoritme. Tak pristop napada so poimenovali napad z posrednikom (ang. Man in the Middle).

Napad s posrednikom je tehnika prestrezanja informacij med izvorom in ciljem. Zamisel samega napada je, da se napadalec vrine med dve žrtvi, ki komunicirata med seboj, z željo prisluškovanja in prestrezanja podatkov. Napadalec se mora obnašati kot posrednik med izvorom in ciljem, pri čemer je lahko uspešen le, če obe žrtvi prepriča, da sporočila posredujeta njemu. Pri tem mora prvo žrtev prepričati, da je on druga žrtev, drugo pa, da je on prva žrtev [Slika 32].



Slika 32 Preprost prikaz napada MITM

Obrazložitev primera iz slike [Slika 33]: Žrtev na levi strani (Victim) želi vzpostaviti varno komunikacijo s strežnikom (Web Server). Napadalčev (Attacker) namen je izvesti napad s posrednikom. Napadalec najprej »zastrupi« tabelo za razreševanje naslovov ARP, s čimer prepriča strežnik, da je on posrednik med strežnikom in ciljem. ARP razreševana tabela je začasna tabela računalnika, ki hrani prevedbe IP naslovov v Ethernet naslove (MAC) [10]. Ko sta obe žrtvi uspešno »zastrupljeni«, lahko napadalec uspešno začne s poslušanjem. Žrtev vzpostavi komunikacijo Web Server, nevedoč, da poteka komunikacija preko napadalca. Tako Web Server posreduje svoj javni ključ napadalcu, napadalec pa svoj javni ključ žrtvi. Napadalec bo lahko s svojim zasebnim ključem dešifriral vse, kar bo poslal žrtvenemu Web Serverju. Napadalec bo lahko vsebino pregledal, obdelal, šifriral z Web Serverjevim javnim ključem in posredoval naprej Web serverju [29].



Slika 33 Preprost prikaz MITM

10.3. Dešifriranje Palo Alto

Mnenje Informacijskega pooblaščenca Republike Slovenije

Ker je dešifriranje in nadziranje prometa izredno občutljiva tema, sem za mnenje obrnil na neodvisen državni organ Informacijski pooblaščenec. Zanimalo me je naslednje: ali obstaja prepoved, omejitev oziroma zakonska ureditev o dešifriranju prometa v lokalnem omrežju, glede na to, da nam sodobne požarne pregrade med drugim omogočajo tudi izvajanje dešifriranje prometa (Man in the middle napad). Vsebina, ki se dešifrira, preveri sumljivo vsebino (AV, spyware, ...), ali podjetje dovoli storitev, ki se skriva znotraj šifrirane povezave. Vsebina se ne shranjuje, pregleduje in podobno.

Odgovor Informacijskega pooblaščenca se glasi: »O prestrezanju HTTPS zahtevkov na posredniškem strežniku (praviloma MITM napadih v podjetjih) je Pooblaščenec letos že izdal nekaj mnenj. Žal še niso objavljena na naši spletni strani, zato vam posredujemo krajši povzetek našega stališča.

Omenjeno prestrezanje je po mnenju Pooblaščenca dovoljeno zgolj izjemoma, ob spoštovanju določenih pogojev. Izvajalec prestrezanja mora v prvi vrsti presoditi, katere podatke želi zbirati oz. hraniti, za kateri namen in za koliko časa. Navedeno mora ustrezno argumentirati, in posameznike, katerih osebni podatki bodo obdelovani, o zbiranju in načinu obdelovanja osebnih podatkov vnaprej ustrezno informirati.

V primeru torej, da je nadzor spletnega prometa utemeljen in nujno potreben, npr. zaradi obravnave varnostnih incidentov, preprečevanja zlorab in napadov na informacijski sistem idr., Pooblaščenec priporoča, da upravljavec o tem predhodno sestavi ali ustrezno dopolni pisni dokument (npr. interni akt, politiko ali pravilnik), v katerem bo natančno opredeljen namen obdelave osebnih podatkov, nabor osebnih podatkov, dostopne pravice do osebnih podatkov in opredeljen postopek uporabe osebnih podatkov. Ta dokument naj tako med drugim vsebuje naslednje informacije:

- kakšen je namen zbiranja in hranjenja podatkov,

- nabor osebnih podatkov, t.j. katere osebne podatke se zbira (IP naslov računalnika v podjetju, naslov ciljnega strežnika, datum, čas, itd);

- koliko časa se omenjeni podatki hranijo, pri čemer mora biti rok hrambe ustrezno kratek glede na namen obdelave podatkov;

- kdo bo imel dostop do teh podatkov in v katerih primerih;

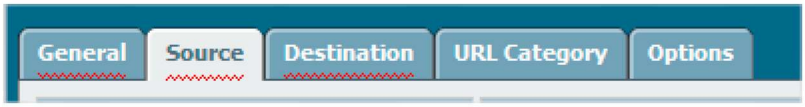
- kakšen bo postopek obravnave teh podatkov (npr. ob preiskovanju vdora, kdo kaj stori...).

Upravljavec mora upoštevati, da gre v primeru nadzora spletnega prometa svojih zaposlenih za hujši poseg v delavčevo komunikacijsko zasebnost, zato mora biti vpogled v tako pridobljene podatke omejen na opisane namene - npr. skeniranje za viruse, oz. vpogled zajetih metapodatkov za potrebe preiskave konkretnega varnostnega incidenta. Vsesplošno pregledovanje tega prometa, ali pregledovanje prometa brez vednosti zaposlenih, po mnenju Pooblaščenca ni v skladu z določili ZVOP-1.« [3]

Ker se vse pogosteje uporabljajo šifrirane povezave, za katerimi se lahko nahaja tudi marsikatera nevarnost ali storitev, nam požarna pregrada omogoča dešifriranje prometa. Da lahko pogledamo, kaj se skriva za šifrirano povezavo, moramo promet dešifrirati. To naredimo s tako imenovanim Man-in-the-middle napadom.

Pri vzpostavitvi varne povezave se vzpostavita dve šifrirani povezavi, od pobudnika komunikacije do požarne pregrade in od požarne pregrade do ciljnega naslova. Tako si požarna pregrada zagotovi, da promet v točki prehoda skozi njo ni več kriptiran, temveč se takoj, ko jo zapusti, ponovno šifrira.

Priprava dešifriranih pravil poteka podobno kot varnostna pravila. Nastavitve se izvajajo na zavihku **Policies->Decription** in so razvrščene v pet osnovnih zavihkov: splošno (ang. General), izvor (ang. Source), cilj (ang. Destination), URL kategorija (ang URL category) in opcije (ang. Options).



Slika 34 Prikaz zavihkov pri kreiranju dešifriranih pravil

Zavihek **General** služi poimenovanju pravila in možnosti kratkega opisa. Na drugem zavihku **Source** se nastavljajo varnostna območja, iz katerih bo šifriran promet prihajal. Poleg splošnega omejevanja na varnostna območja lahko izvorno območje omejimo še na enoznačni IP naslov, območje naslovov, celo na uporabnika.

Na zavihku Destination se nastavlja smer, v katero je šifriran promet namenjen. Tudi tu se nastavlja varnostno območje, dodatno pa se lahko omeji še na enoznačni IP naslov ali območje naslovov. Pri **URL Category** se nastavlja, na katere kategorije spletnih naslovov naj se aktivira pravilo. Če želim, da se pravilo aktivira na Facebook, Twitter, LinkedIn in podobno, bi v URL Category izbral social-networing. Na zadnjem zavihku **Options pa** se nastavljajo akcije in tip dešifriranja.

Poleg akcij **Decrypt** in **No Decrypt**, lahko nastavljamo še tip dešifriranja Forward-Proxy in Inbound Inspection. Namen akcije **Decrypt** je, da želimo promet, ki se bo ujemal s pripravljenim pravilom, dešifrirati in obratno za **No Decrypt.** Tip **Forword-proxy** se uporablja, ko uporabnik dostopa do varnih HTTPS strani, na primer ko uporabnik v brskalnik https://www.youtube.com.

Tip Inbound Inspection pa se uporablja takrat, ko tretje osebe dostopajo do naših strežnikov po varni povezavi. Pri takšni nastavitvi je potreben certifikat, ki je nameščen na strežniku, namestiti tudi požarno pregrado, saj bo le tako lahko dešifriral povezavo.

Pri dešifriranju prometa je smiselno upoštevati nekaj nasvetov iz prakse:

- Dešifriranje naj se ne bi izvajalo za varne lokalne storitve in uporabnike, finančnih storitev in neznane URL kategorij.
- Poizkušamo se izogibati splošnih (ang. Any) nastavitev na zavihkih Source in Description.

10.3.1. 7. naloga: priprava dešifriranega pravila

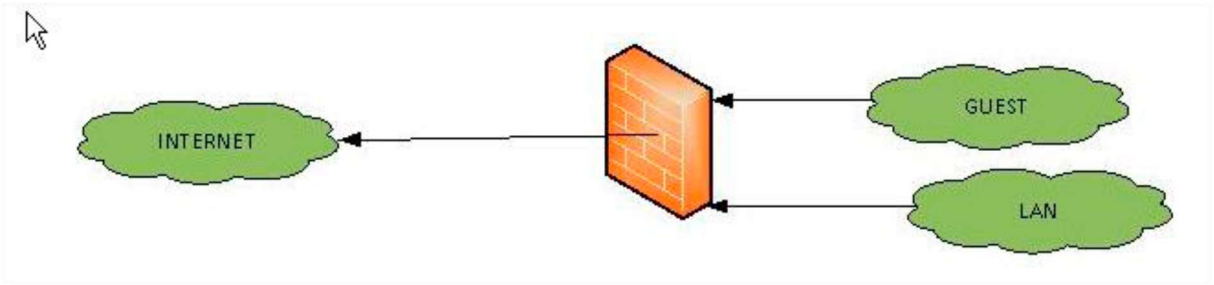
Prijavi se na spletno storitev gmail.com in preveri, če požarna pregrada prepozna storitev. Pripravi pravilo, ki bo blokiralo celotno storitev Gmail Base in preveri, če pravilo učinkuje. V naslednjem koraku poizkusi blokirati samo storitev g-talk znotraj brskalnika. V zadnjem koraku poizkusi prenesti testni virus iz spletnega naslova https://www.eicar.org/download/eicar.com.

Praktični del

11. Rešitve

11.1. 1. naloga: priprava topologije omrežja majhnega podjetja

Pripravi topologijo omrežja majhnega podjetja. Podjetje dela z večjim številom zunanjih strank, ki so za omrežje tvegana, ima pa tudi lastne zaposlene. V svetovni splet se povezujejo preko ADSL povezave. Omrežje smiselno loči na tri podomrežja. Glede na pripravljeno topologijo, umesti požarno pregrado v shemo. Dopolni shemo tako, da omrežja, ki se vklapljajo na požarno pregrado smiselno poimenuješ z imeni Guest, Lan in Internet. Imena bodo pozneje uporabljena za pripravo varnostnih območij.

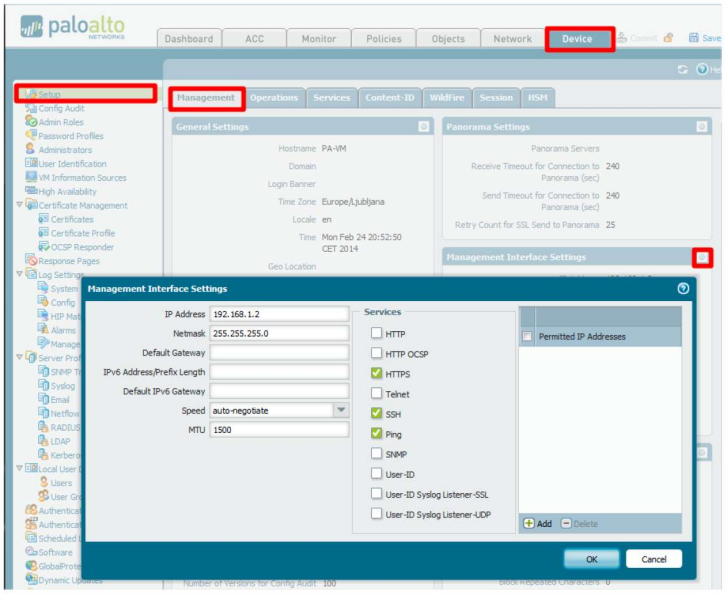


Slika 35 Prikaz izgleda omrežja

11.2. 2. naloga: priprava osnovni nastavitev za dostop in konfiguracijo požarne pregrade

Na požarni pregradi spremeni privzeti IP naslov upravljalnega vmesnika (managment interface).

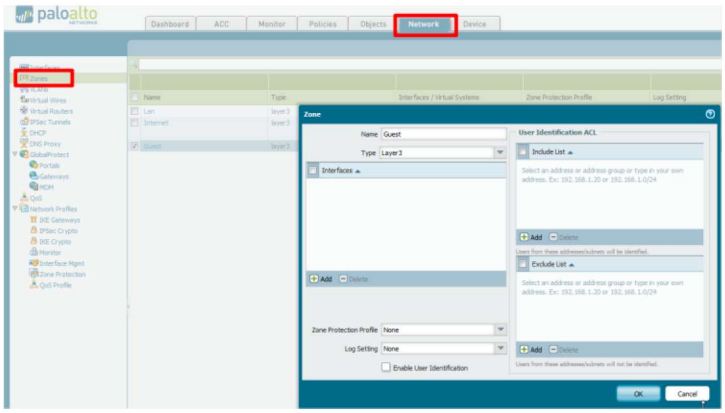
V mojem primeru bo naslov za upravljanje 192.168.1.2 z masko 24. Naslov nastavim na zavihku Device -> Setup -> Managment -> Managment interface Setting. V okvirju Services nastavim možnosti, na katere storitve se bo upravljalni del odzival. Polje Permitted IP Addresses je namenjeno omejevanju naslovov, ki lahko dostopajo do upravljalnega vmesnika. Če polj ne izpolnimo, pomeni, da upravljavski vmesnik nima dostopnih omejitev na IP naslov.



Slika 36 Prikaz priprave managment naslova naprave

a.) Za vse tri segmente (Guest, Lan, Internet) pripravi varnostna območja.

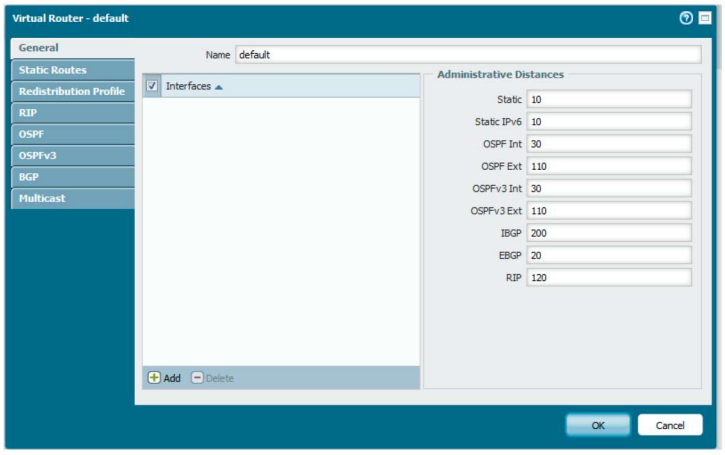
Vsa varnostna območja, v katere bom razvrstil omrežja, bodo v Layer 3 postavitvi. Varnostna območja poljubno in smiselno poimenujem. Nastavitve se izvajajo na zavihku Network ->Zones. Vsak od treh segmentov Guest, Lan in Internet bo tipa Layer 3 (polje TYPE). Polje Interfaces pustim neizpolnjeno, nastavil ga bom, ko bom nastavljal vmesnike.



Slika 37 Prikaz priprave varnostnih območij

b.) Za segment Guest pripravi avtomatsko dodeljevanje enoznačnih IP naslovov v območju med 10.20.20.100 in 10.20.20.200. Pri tem si pomagaj s privzetim prehodom 10.20.20.1, primarnim (193.189.177.55) in sekundarnim (193.189.160.23) DNS-jem. Vmesnik Ethernet1/1 naj se odziva na naslov 192.168.1.1 z masko 255.255.255.0 (je del varnostnega območja Lan). Vmesnik Ethernet1/2 naj bo nastavljen za vzpostavitev povezave PPPoE (je del varnostnega območja Internet), na vmesnik Ethernet1/3 nastavi, da bo poslušal na naslovu 10.20.20.1 z masko podomrežja 255.255.255.0 (je del varnostnega območja Guest). Ne pozabi, da mora vsak vmesnik imeti usmerjevalno tabelo.

Virtualne usmerjevalne tabele se nastavljajo na zavihku Network->Virtual Router. Najprej pripravim virtualni usmerjevalnik z imenom Default. V levem delu okna pod oznako General ga poimenujem. Virtualni usmerjevalnik (ang. Virtual Ruter) se poskuša sam naučiti usmerjevalnih pravil. Pravil, ki se jih naprava ne zna sama naučiti, lahko pozneje sami dopolnimo. To storim tako, da jih dodam na zavihku Static Routes. Pri večini preprostih namestitev požarnih pregrad se uporablja le en navidezni usmerjevalnik.



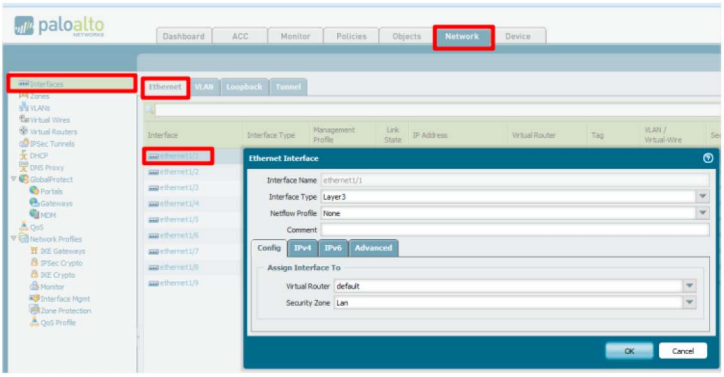
Slika 38 Prikaz priprave virtualnega usmerjevalnika

Priprava vmesnikov

Pripraviti moram še tri vmesnike. Vsakemu od vmesnikov bom dodelil svojo varnostno območje, navidezni usmerjevalnik in enoznačni IP naslov. Nastavitev vmesnikov bom izvedel na zavihku Network->Interfaces->Ethernet.

Ethernet1/1

Eth1/1 bo v varnostnem območju Lan in ima naslovni prostor 192.168.1.0/24.



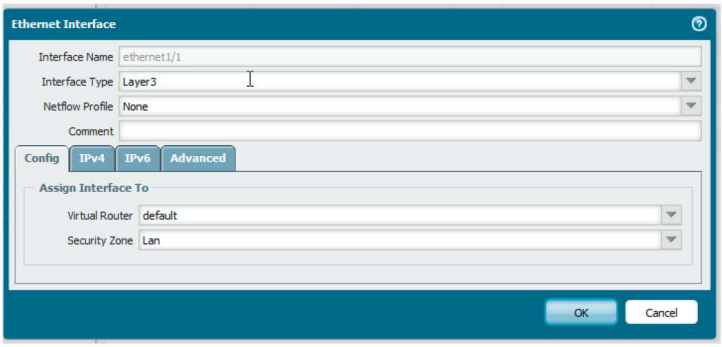
Slika 39 Prikaz priprave vmesnikov

Nastavitve za Ethernet1/1

Zavihek Config: Interface type: Layer 3

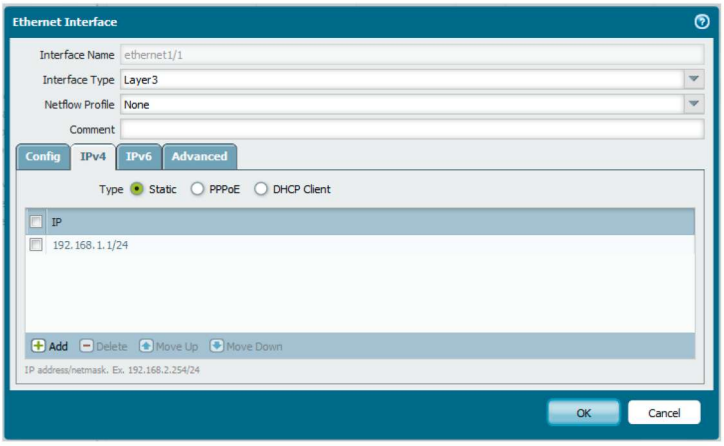
Virtual Router: Default

Security Zone: Lan



Slika 40 Prikaz priprave vmesnika

Zavihek IPv4: nastavimo IP vmesnik in masko



Slika 41 Prikaz priprave vmesnika

Postopek ponovim še za Ethernet1/2, Ethernet1/3, s tem, da: Ethernet1/2 bo v varnostnem območju Internet, naslov ima dodeljen s strani internetnega ponudnika (ISP-ja) in ima MGMT profil.

Zavihek Config: Interface type: Layer 3

Virtual Router: Default

Security Zone: Internet

Zavihek IPv4: nastavimo PPPOE (vnesemo uporabniške podatke za povezavo z internetnim ponudnikom).

Ethernet 1/3 bo v varnostnem območju Lan, ki ima naslovni prostor 10.20.20.0/24 in ima MGMT profil.

Zavihek Config: Interface type: Layer 3

Virtual Router: Default

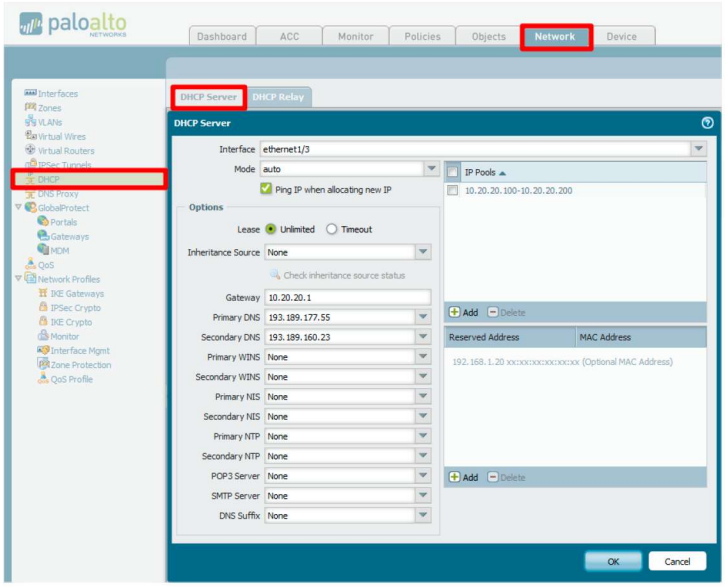
Security Zone: Lan

Zavihek IPv4: nastavim naslov vmesnika 10.20.20.1 in masko podomrežja 24 (10.20.20.1/24).

Priprava DHCP serverja

Avtomatsko dodeljevanje enoznačnih IP naslovov se nastavlja na zavihku Network->DHCP->DHCP servers. Za avtomatsko dodeljevanje naslovov v varnostnem območju Guest moram nastaviti DHCP server, to izvedem na Ethernet1/3. Privzet prehod nastavim na 10.20.20.1, kar je vmesnik Ethernet1/3. Nastavim še območje dodeljevanja enoznačnih IP naslovov (ang. IP

Pools). Območja enoznačnih IP naslovi so naslovi, ki jih bo DHCP server dodeljeval odjemalcem. Primarni in sekundarni DNS naslov sta lahko katerikoli DNS naslov, v mojem primeru bom izbral javna DNS naslova mojega ponudnika internetnih storitev, 193.189.177.55 in 193.189.160.23 [Slika 42].



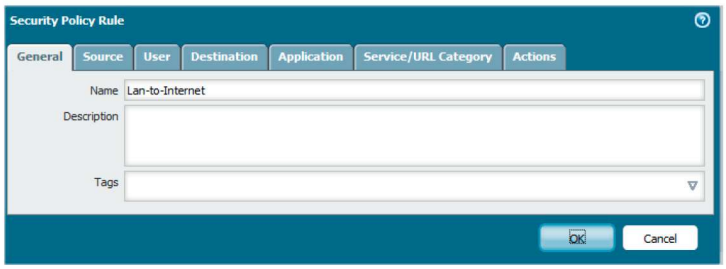
Slika 42 Prikaz priprave DHCP stržnika

11.3. 3. naloga: priprava varnostnih pravil

Pripravi varnostna pravila, ki bodo dovoljevala promet iz varnostnega območja: Lan proti Guest, Lan proti Internet, Guest proti Internet, omogoči vsaj storitve HTTP (vrata 80), HTTPS (vrata 443), med vsemi varnostnimi območji dovoli aplikacijo ping, razen iz območja Guest proti Lan. Preveri, katere nastavitve ne delujejo in zakaj.

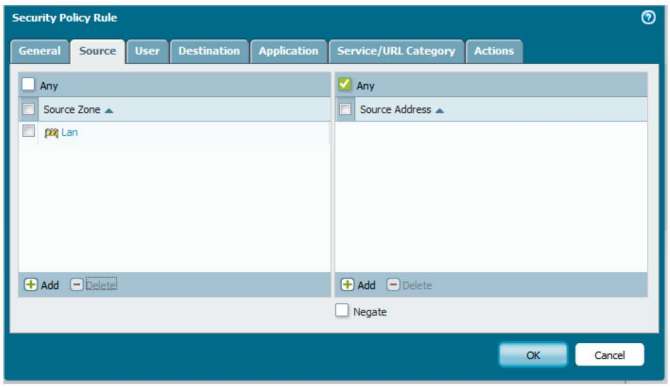
Naprava privzeto zavrača promet na vseh vmesnikih, razen na upravljalnem vmesniku. Za pravilno delovanje potrebujem splošno varnostno pravilo, ki bo dovoljevalo promet iz kateregakoli varnostnega območja v katerokoli varnostno območje. Varnostna pravila se nastavljajo na zavihku Policies->Security. Varnostno pravilo smiselno poimenujem. Postopek priprava varnostnega pravila je sledeč:

- Na zavihku General pravilo smiselno poimenujem z Lan-to-Internet.



Slika 43 Prikaz priprave varnostnega pravila

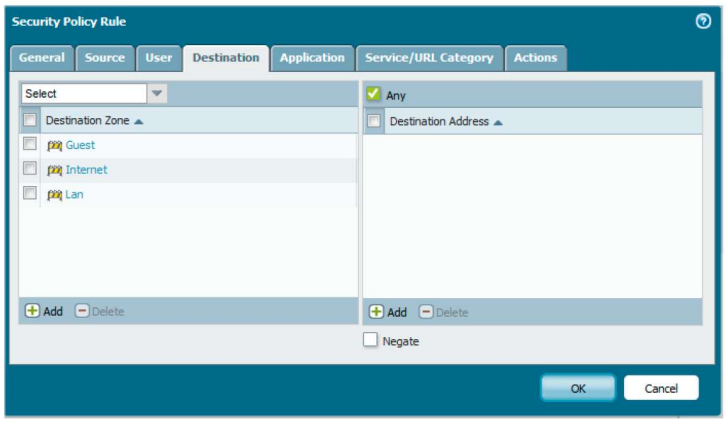
- Na Source zavihku nastavim varnostna območja, iz katerih bo prihajal promet in naslove, za katere se bo pravilo ujemalo. V mojem primeru nastavim Security Zone na Lan in Source address na ANY.



Slika 44 Prikaz priprave varnostnega pravila za izvor

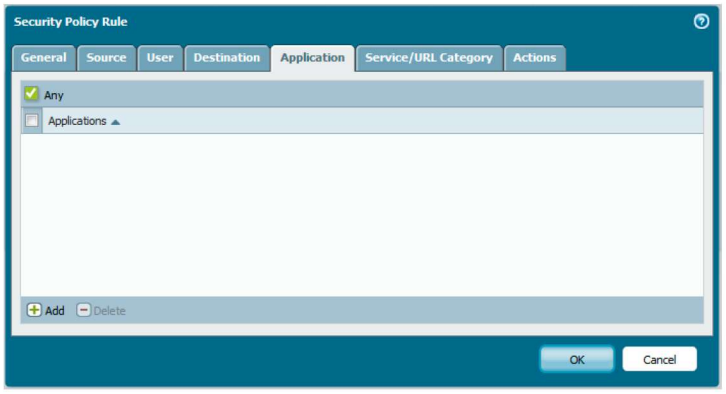
- V kolikor bi imel nastavljeno prepoznavanje uporabnikov, bi lahko na zavihku User omejil ali dovolil samo določene uporabnike in/ali omejil ali dovolil glede na operacijskih sistemih, nameščenost antivirusnega programa, ali ima uporabnik šifriran disk itd (HIP Objects). V mojem primeru nastavim User in HIP Object na ANY.

- Na zavihku Destination je nastavitev podobna kot pri Source-u, s tem, da se sklicujemo na ciljno varnostno območje in naslove, kamor je promet namenjen. Tu nastavim na ANY.



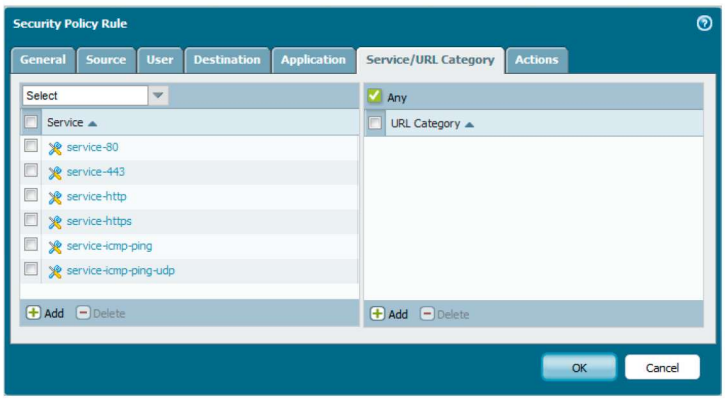
Slika 45 Prikaz priprave varnostnega pravila za cilj

- Na zavihku Application omejim ali dovolim na tip aplikacije (Gmail, Gmail Base, Gmail Chat, web-browsing,..), ki jih bom dovolil ali zavrnil ob prepoznavi. V mojem primeru se bom z omejevanjem aplikacije ukvarjal pozneje, zato za zdaj nastavim na ANY.



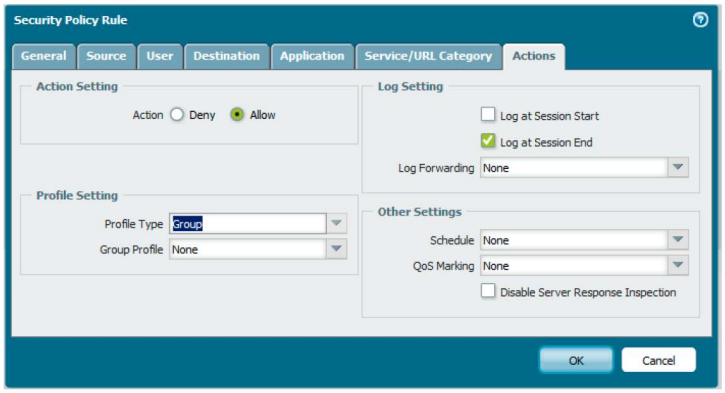
Slika 46 Prikaz priprave varnostnega pravila za aplikacije katere bo naprava zavračala ali dovoljevala

- Na zavihku Service/URL Category nastavim, katere storitve dovolim ali zavračam. Promet, ki je bil zajet, lahko omejim glede na kategorijo (npr. če obiščem spletno stran soundcloud.com, bo naprava prepoznala, da gre za kategorijo Music). Tu nastavil vrata 80 IN 443, HTTPS, HTTP in ping.



Slika 47 Prikaz priprave varnostnega pravila za storitve katere bo naprava zavračala ali dovoljevala

- Na zavihku Actions nastavim želeno akcijo v primeru ujemanja. V primeru izbire Action Setting Allow bo naprava promet, ki bo ustrezal pogojem, nastavljenim v prejšnjih zavihkih, dovolila oziroma sprejemala, v primeru izbire Deny pa zavračala. Nastavitev Profile Type pustim za pozneje. Nastavitev Profile Type-a omogoča, da na pravilo vežemo tudi preverjanje, kot so virusi, Anti-Spyware, zlonamerno kodo, URL filtriranje, blokiranje datotek in iskanje posebnega vzorca v vsebini datoteke. V polju Log Setting nastavim še trenutek beleženja prometa. Trenutek beleženja je čas, v katerem želim ustvariti zapis v dnevniški zapis. Tu lahko izbiram med začetkom seje (ang. Log at Session Start) ali koncu seje (ang. Log at Session End). Beleženje seje nastavim na Log at Session End.



Slika 48 Prikaz priprave varnostnega pravila, zaključne nastavitve

Postopek ponovim še za varnostno območje Guest, pri tem spremenim:

- Na zavihku General poimenujemo pravilo Guest-to-Internet
- Na zavihku Source namesto Lan nastavim Guest varnostno območje
- Na zavihku Destination nastavim samo varnostno območje Internet

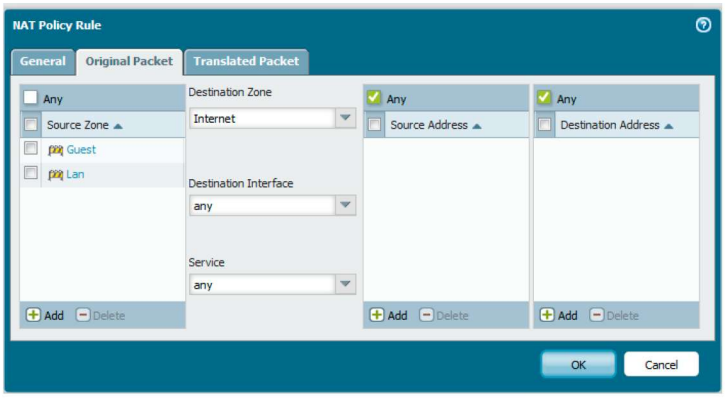
Trenutna nastavitev požarne pregrade mi ne omogoča povezljivosti z internetom oziroma z varnostnim območjem Internet. Manjka mi preslikava enoznačni naslovov v javni naslov.

11.4. 4. naloga: priprava preslikovalnega pravila

Požarni pregradi pripravi preslikovalno pravilo, ki bo omogočalo komunikacijo naprav z internetom. Preslikovanje naj se izvaja na vseh lokalnih naslovov iz vseh varnostnih območij v naslov, ki je dodeljen napravi s strani ponudnika internetnih storitev.

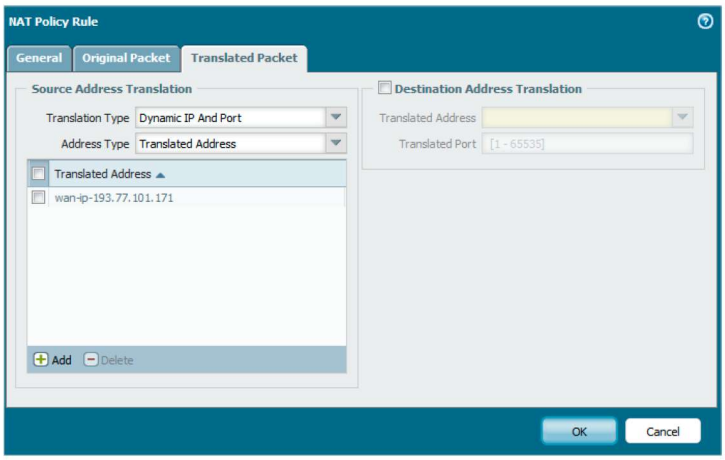
Ker privatni naslovi, kot sta v mojem primeru 192.168.1.0/24 in 10.20.20.0/24, »ne obstajajo« v javnem naslovnem prostoru oziroma ob prehodu iz lokalnega omrežja v svet, prvi usmerjevalnik zavrže naslov z izvornim naslovom (192.168.1.0/24, 10.20.20.0/24,…), moram pretvoriti izvorni naslov v naslov, ki mi ga je dodelil ponudnik internetnih storitev. Te nastavitve izvedem na zavihku Policies-> NAT.

Na zavihku General pravilo najprej smiselno poimenujem. Ker vem, da želim preslikovanje izvesti na prometu, ki potuje iz varnostnega območja Guest in Lan proti Internetu, lahko rečem, da je moj izvor prometa Guest in Lan, cilj pa Internet. Iz tega sledi, da na zavihku Original Package v polju Source Zone izberem Guest in Lan, v Destination pa Internet. Ostale nastavitve na tem zavihku lahko pustim nastavljene na ANY.



Slika 49 Prikaz nastavitve preslikovalnega pravila

Na zavihku Translated package nastavim, kako in v kaj se bo pretvoril izvorni naslov. Tako v Translated Type izberem možnost Dynemic IP and Port, v Address Type Translated Address in v polju Translated Address vnesem svoj javni enoznačen IP naslov, dodeljen s strani ponudnika interneta. Požarna pregrada bo tako vsak naslov, ki se bo ujemal z prej nastavljenim pravilom ne glede na vrata, preslikala v javni naslov.



Slika 50 Prikaz nastavitve preslikovalnega pravila

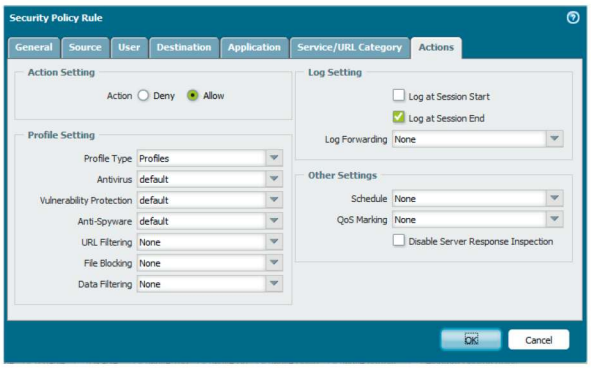
11.5. 5. naloga: priprava pravila za preprečevanje ranljivega prometa

Obišči spletno stran (http://www.eicar.org/download/eicar.com) in si prenesi okuženo datoteko. Omenjena spletna stran mi omogoča prenos testnega primerka virusa, ki ne škoduje računalniku.

Ali naprava prepozna okuženo datoteko? Umesti anti-spyware protection, antivirus protection in Vulnerability Protection v najbolj smiselno varnostno pravilo, ki je namenjeno komuniciranju s svetom. Ponovno preveri na isti spletni strani, če sedaj varnostni profili delujejo.

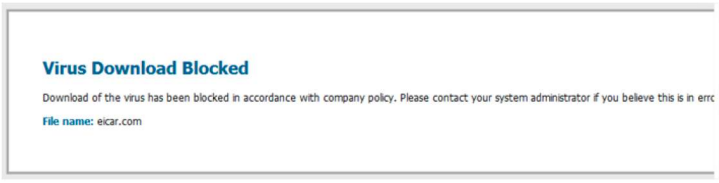
Ob obisku strani mi požarna pregrada ne sporoči nobene nevarnosti, ker na nobenem varnostnem pravilu nimam nastavljenega preverjanja škodljivosti prometa. Požarna pregrada ima privzeto prednastavljene profile za antivirus anti-spayware in Vulnerability Protection, kar bo zadostovalo za testni primer.

Poskrbeti moram, da anti-spyware protection, antivirus protection in vulnerability protection profile nastavim na varnostni pravili Lan-to-Internet in Guest-to-Internet. To izvedem na zavihkih, kjer sem pripravljal varnostna pravila, in sicer tako, da kliknem na varnostno pravilo Lan-to-Internet in na zadnjem zavihku Action pri poljih anti spyware protection, antivirus protection in vulnerability protection, nastavim na vrednosti Default, kakor so poimenovani privzeti varovalni profili.



Slika 51 Prikaz dodajanja varnostnih profilov na pravila

Ob ponovnem obisku strani mi ne dovoli prenesti datoteke z opozorilom in zabeležko v dnevniku.



Slika 52 Prikaz sporočila o odkriti grožnji in njeni blokadi

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action
	04/21 13:10:57	virus	Eicar Test File	Internet	Lan	188.40.238.250		192.168.1.142	51338	web-browsing	deny
	04/21 13:07:15	virus	Eicar Test File	Internet	Lan	188.40.238.250		192.168.1.142	51259	web-browsing	deny
	04/21 13:07:09	virus	Eicar Test File	Internet	Lan	188.40.238.250		192.168.1.142	51255	web-browsing	deny
	02/28 22:49:46	virus	Eicar Test File	Internet	Lan	188.40.238.252		192.168.1.113	52950	web-browsing	deny

Slika 53 Prikaz blokade grožnje v dnevniškem zapisu

11.6. 6. naloga: prepoznava aplikacije

Dopolni varnostna pravila tako, da:

se iz varnostnega območja Lan proti Guest dovoli aplikacija MS-RDP. Preveri ali se komunikacija vzpostavi. Poizkusi vzpostaviti povezavo z oddaljenim računalnikom po vratih 3388. Za vzpostavitev oddaljene povezave uporabi program Microsoft Terminal Services (start->mstsc.exe), za vzpostavitev povezave po drugih vratih pa z sintakso »IP naslov:3388« se iz varnostnega območja Lan proti Internetu onemogoči aplikacijo Gmail in preveri. V drugem koraku popravi varnostno pravilo in onemogoči samo Gmail Chat. Kaj se zgodi in zakaj?

Če poizkušam vzpostaviti povezavo z računalnikom v Guest varnostnem območju, se povezava ne vzpostavi, v dnevnik pa se zapiše, da je zadnje pravilo pravilo, ki zavrača vse ustrezalo prometu, kot kaže spodnja slika.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
	06/01 20:30:43	end	Lan	Guest	192.168.1.142		10.20.20.3	3389	incomplete	deny	default	62
	06/01 20:30:37	end	Lan	Guest	192.168.1.142		10.20.20.3	3389	incomplete	deny	default	132

Slika 54 Prikaz zavračanja prometa

Za vzpostavitev oddaljene povezave moram pripraviti novo pravilo, ki reagira na promet, ki bo prihajal iz varnostnega območja Lan in potovalo proti Guest območju, dovoljenje za prehod pa bo imela samo aplikacija MS-RDP, kot kaže slika [Slika 54].

	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
4	Lan-Guest-RDP	none	Lan	any	any	any	Guest	any	ms-rdp	application-default

Slika 55 Prikaz dodanega novega pravila za vzpostavitev oddaljene povezave

Iz dnevnika zapisov vidim, da je ob poizkusu vzpostavitve povezave preko mstsc.exe oziroma programa Microsoft Terminal Service požarna pregrada v prometu uspešno prepoznala aplikacijo, s katero sem vzpostavil povezavo. Kljub temu, da se poizkušam povezati s programom po drugih vratih (vrata 3380), požarna pregrada ne blokira prometa.

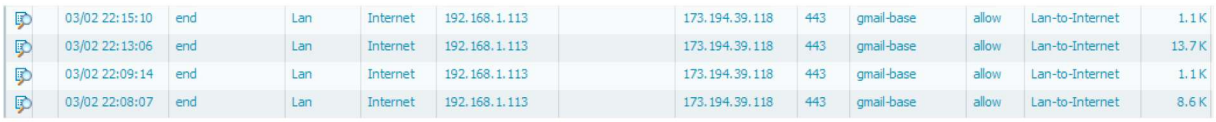
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
	06/01 20:30:43	end	Lan	Guest	192.168.1.142		10.20.20.3	3389	ms-rdp	allow	Lan-Guest-RDP	62
	06/01 20:30:37	end	Lan	Guest	192.168.1.142		10.20.20.3	3389	ms-rdp	allow	Lan-Guest-RDP	132
	06/01 17:35:19	end	Lan	Guest	192.168.1.142		10.20.20.3	3380	ms-rdp	allow	Lan-Guest-RDP	62
	06/01 17:35:13	end	Lan	Guest	192.168.1.142		10.20.20.3	3380	ms-rdp	allow	Lan-Guest-RDP	132

Slika 56 Prikaz iz dnevniškega zapisa, da naprava ne blokira več oddaljene povezave

11.7. 7. naloga: priprava dešifriranega pravila

Prijavi se na spletno storitev gmail.com in preveri, če požarna pregrada prepozna storitev. Pripravi pravilo, ki bo blokiralo celotno storitev Gmail-Base in preveri, če pravilo učinkuje. V naslednjem koraku poizkusi blokirati samo storitev g-talk znotraj brskalnika. V zadnjem koraku poizkusi prenesti testni virus iz spletnega naslova https://www.eicar.org/download/eicar.com.

Ob prijavi na spletno storitev gmail.com požarna pregrada prepozna aplikacijo kot Gmail Base.



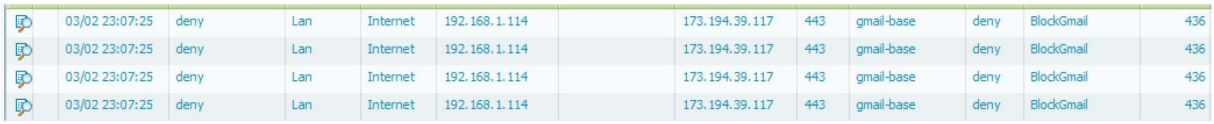
	03/02 22:15:10	end	Lan	Internet	192.168.1.113		173.194.39.118	443	gmail-base	allow	Lan-to-Internet	1.1 K
	03/02 22:13:06	end	Lan	Internet	192.168.1.113		173.194.39.118	443	gmail-base	allow	Lan-to-Internet	13.7 K
	03/02 22:09:14	end	Lan	Internet	192.168.1.113		173.194.39.118	443	gmail-base	allow	Lan-to-Internet	1.1 K
	03/02 22:08:07	end	Lan	Internet	192.168.1.113		173.194.39.118	443	gmail-base	allow	Lan-to-Internet	8.6 K

Slika 57 Prikaz prepoznane aplikacije Gmail Base

Kot je prikazano na zgornji sliki [Slika 57], promet potuje iz Lan proti Internet varnostnemu območju, pri tem pa uporablja varno komunikacijo na vratih 443. Za blokiranje prometa Gmail Base moram pripraviti novo pravilo, ki bo zavračalo promet, ki bo prihajal iz varnostnega območja Lan in potoval Internetu ter reagiral na Gmail Base aplikacijo.

Slika 58 Prikaz blokiranega pravila za aplikacijo Gmail Base

Ko po blokiranem pravilu ponovno poizkusim obiskati spletno storitev gmail.com, se ta ne odziva več, v dnevnik zapisov pa požarna pregrada zapiše, da je zavrnila ves promet, ki je bil identificiran kot Gmail Base.

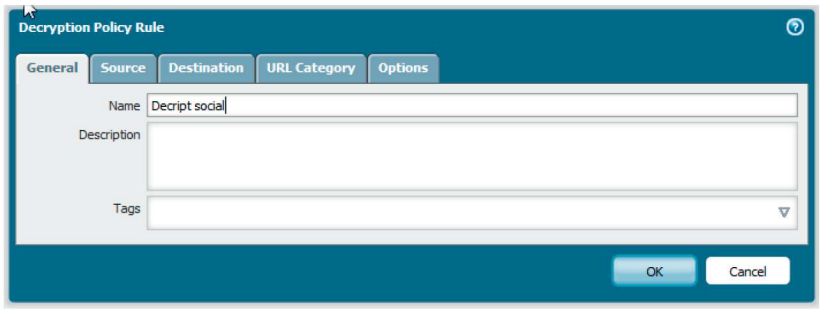


	03/02 23:07:25	deny	Lan	Internet	192.168.1.114		173.194.39.117	443	gmail-base	deny	BlockGmail	436
	03/02 23:07:25	deny	Lan	Internet	192.168.1.114		173.194.39.117	443	gmail-base	deny	BlockGmail	436
	03/02 23:07:25	deny	Lan	Internet	192.168.1.114		173.194.39.117	443	gmail-base	deny	BlockGmail	436
	03/02 23:07:25	deny	Lan	Internet	192.168.1.114		173.194.39.117	443	gmail-base	deny	BlockGmail	436

Slika 59 Prikaz iz dnevniškega zapisa, da je požarna pregrada blokirala Gmail Base

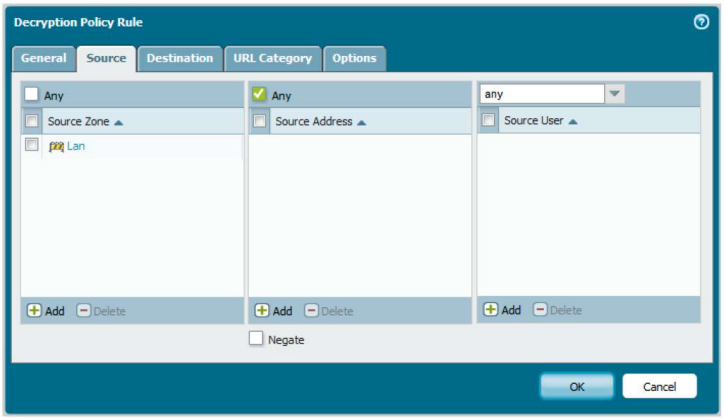
Če želim blokirati samo storitev znotraj varne povezave, moram najprej pripraviti dešifrirano pravilo. Pravilo bo poskrbelo, da bom lahko nadziral tudi šifriran promet. Za dešifriranje odhodnega prometa moram pripraviti novo dekripcijsko pravilo (ang. Decription Policy Rule), ki se nahaja na zavihku Policies->Decription.

V prvem koraku pravilo smiselno poimenujem [Slika 60], pri pripravi pravila v Decryption Policy Rule pa se v celoti izognem nastavitvi ANY.



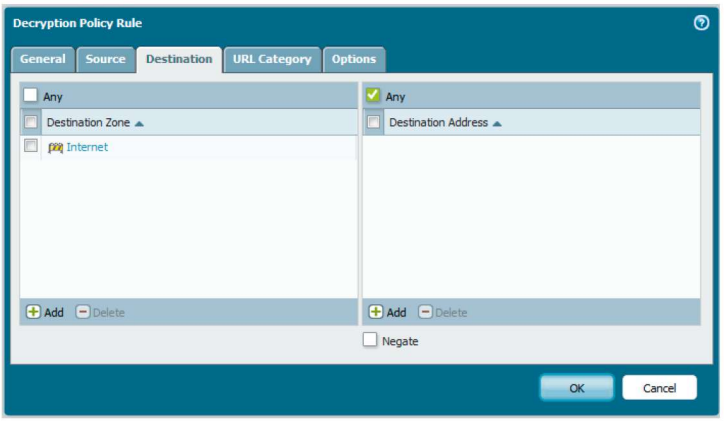
Slika 60 Prikaz priprave dešifriranega pravila

Na zavihku Source določim varnostno območje, iz katerega bo promet prihajal. Tu izberem varnostno območje Lan. Poleg izvornega varnostnega območja lahko tukaj omejim izvor še na določene enoznačne IP naslove, sklope domen, morebitne prepoznane uporabnike.



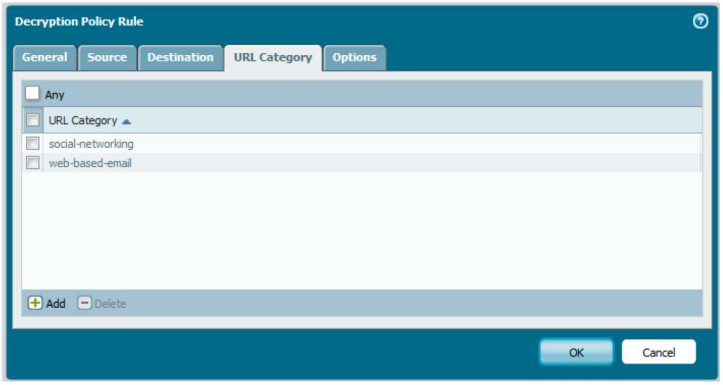
Slika 61 Prikaz priprave dešifrirnega pravila za izvor

Na zavihku Destination nastavim varnostno območje, v smeri, v kateri potuje promet. Tako na zavihku Destination nastavim na varnostno območje Internet. Poleg tega lahko v kategoriji Destination Address omejim ciljno območje na točno določen naslov ali skupino naslovov.



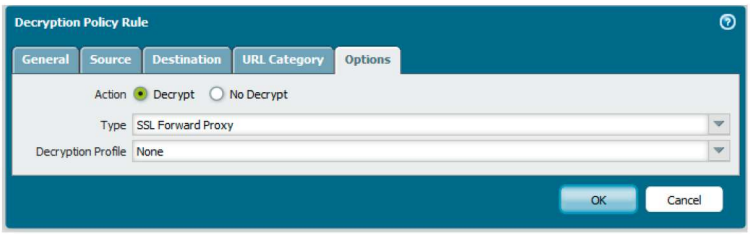
Slika 62 Prikaz priprave dešifriranega pravila za cilj

Na zavihku URL Category nastavim za katere kategorije naj naprava dešifrira promet. Ker sem si zbral Gmail, izberem web-based-email in social-networking [Slika 63].



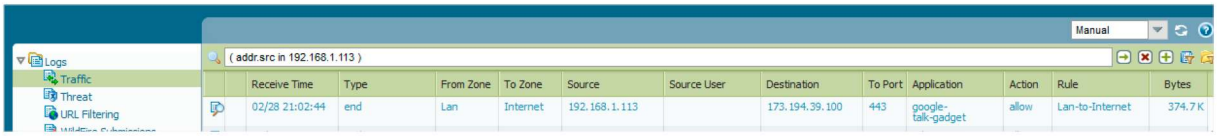
Slika 63 Prikaz priprave dešifriranega pravila za kategorije, na katere bo pravilo reagiralo

Na zadnjem zavihku izberem tip dešifriranja (Type) in akcijo (Action), za katero želim, da se izvede v primeru ujemanja pravila. V mojem primeru bom dešifriral odhodni promet, zato izberem SSL Forward Proxy.



Slika 64 Prikaz zadnjega koraka pri pripravi dešifrirnega pravila

Ob ponovnem obisku spletnega naslova gmail.com, se v dnevniške zapise zapiše zapis, ki nakazuje na prepoznano spletno storitev Google Talk oziroma G-Talk.



Slika 65 Prikaz prepoznane aplikacije po uspešni dekripciji prometa

V kolikor želim blokirat prepoznani G-Talk, moram pripraviti novo varnostno pravilo. Novo varnostno pravilo bo iz katerega koli izvornega varnostnega območja v katerokoli ciljno varnostno območje blokiralo Google Talk, kot prikazuje slika 70.

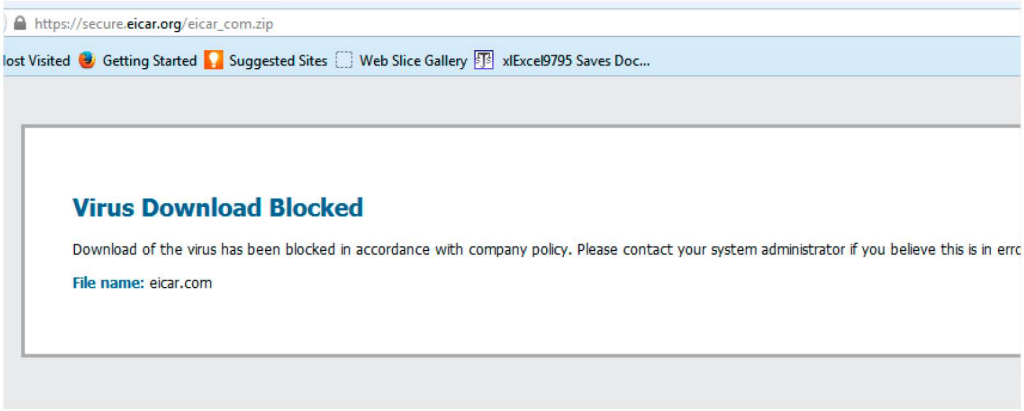
Slika 66 Prikaz pravila, bo blokiralo na novo prepoznano aplikacijo

Ob uveljavitvi pravila dnevniški zapis pokaže, da je bila aplikacija uspešno blokirana.

	02/28 22:48:23	deny	Lan	Internet	192.168.1.113		173.194.39.103	443	google-talk-gadget	deny	Blokiraj kriptirane	155.0 K
	02/28 22:48:23	deny	Lan	Internet	192.168.1.113		173.194.39.102	443	google-talk-gadget	deny	Blokiraj kriptirane	266.2 K

Slika 67 Prikaz blokiranega dešifriranega prometa aplikacije google-talk-gadget

Z obiskom spletnga naslova https://www.eicar.org/download/eicar.com želim preveriti ali me požarna pregrada varuje pred virusi, ki so za varno povezavo. Opazim, da mi požarna pregrada prepreči prenos programa, ker je datoteka okužena.



Slika 68 Prikaz sporočila o odkriti grožnji pri HTTPS in njeni blokadi

12. Sklepna ugotovitev

V diplomski nalogi želim bralcu prikazati postopke osnovno nastavitev. To storim skozi teoretični del, ki mu da osnovne temelje za poznavanje naprave oziroma mu osveži poznavanje požarne pregrade naslednje generacije Palo Alto VM-300, ta del pa je nadgrajen s praktičnim.

Ključnih aspektov praktičnega dela diplomske naloge je več. Osredotočil sem se na umestitev požarne pregrade v lokalno omrežje, pripravo osnovnih nastavitev požarne pregrade, kot so delovale požarne pregrade prve, druge in tretje generacije, prikaz delovanja principov delovanja požarnih pregrad četrte generacije, in s tem bralcu približati razumevanje delovanja požarnih pregrad naslednje generacije. Naprava ima sicer še precej več dodatnih možnosti delovanja in nastavitev, kot so zapisane v tej diplomski nalogi. Navedene zadostujejo za najbolj nujno zaščito omrežja.

Diplomska naloga ob smiselnem prepletu teoretičnega in praktičnega dela uporabnika vodi do uspešne povezanosti in zaščite s svetovnim spletom in z lokalnimi omrežji. Da je bila zaščita lokalnega omrežja resnično uspešna, lahko preverimo s preprostim korakom – prenos testnega primerka virusa, ki v tem primeru ne škodi. Ob pisanju sem predpostavljal, da tisti, ki se odloča za uporabo požarne pregrade Palo Alto, deluje v okolju, polnem zlonamernih kod in vsiljivcev, zato je testiranje nastavitev nujno.

Prav tako je nujno vedenje, kaj nam nastavljene varnostne politike dopuščajo oziroma onemogočajo, zato ena od nalog od uporabnika želi preverjanje delovanje določenih aplikacij (Gmail Chat, MS-RDP). S tem bom vstopil na področje kriptologije in njej povezanim vedam. Pomemben segment pri tem ima tudi prepoved oziroma omejitev dešifriranja prometa v lokalnem omrežju, pri čemer sem se za mnenje obrnil tudi na institucijo Informacijskega pooblaščenca. Po besedah omenjene institucije, mora izvajalec prestrezanja v prvi vrsti presoditi, katere podatke želi zbirati oziroma hraniti, kakšen je njihov namen in koliko časa jih želi zbirati. Poleg ustreznih argumentov mora navesti tudi, kateri osebni podatki bodo obdelani, kdo bo do njih lahko dostopal in podobno, ter o tem vnaprej ustrezno informirati. To kaže na to, da lahko namestitev požarne pregrade tudi prekorači mejo zasebnosti, zato je nujna opredelitev področja delovanja in seznanitev vseh vpletenih. To področje varujejo tudi določila ZVOP-1.

Omenjeno področje o informiranju posameznikov, ki jih upravljavci požarne pregrade zajamejo v svoje »analize«, dobiva vse večjo veljavo in bi ga bilo v celoti vredno zapisati v obliki diplomske naloge. Namreč, kljub temu da nam požarna pregrada daje zadostno varnost, pa po drugi strani lahko trpijo uporabniki, priključeni na lokalno omrežje.

Prikaz upravljanja požarne pregrade s pomočjo nalog v diplomski nalogi daje bralcu, željnemu poglobljenega raziskovanja, lažji prehod na višji nivo upravljanja.

Eden od ciljev diplomske naloge je bil pripraviti koncept vaj, ki bi se lahko izvajale prek virtualnega laboratorija tako, da bi si eno ali nekaj naprav delilo veliko število inženirjev. Cilj sem dosegel, zato lahko upravičeno rečem, da bi moje delo lahko koristilo podjetjem, ki se ukvarjajo z izvajanjem tečajev z požarno pregrado Palo Alto.

Zavedanje o potrebi po dobri zaščiti je vse večje, k temu se nagiba tudi vse več slovenskih podjetij. Kot sem v uvodu zapisal, je Palo Alto nedavno razkril rekordne poslovne rezultate, novice pa sovpadajo tako z vse večjim zavedanjem o nujnosti dobre zaščite pred vsiljivci kot tudi vse pogostejšimi vdori v računalniške sisteme. Želim si, da bo moja diplomska naloga lahko tistemu, ki bo želel uporabljati Palo Alto požarno pregrado, dala čim več znanja in smernic za ustrezno rokovanje z napravo.

13. Literatura

[1] Palo Alto: Palo Alto networks administratr's guide, Dostopno na: http://digitalscepter.com/wp-content/uploads/PAN-Guides/Palo-Alto-3.1_Administrators_Guide.pdf

[2] Chris Brenton, Bob Abuhoff, Andrew Hamilton: Mastering-Cisco-Routers (2005), Založba Sybex, poglavje 3,4

[3] Mnenje informacijske pooblaščenec Republike Slovenije, odgovor v elektronskem sporočilu 08/2014, g. Igor Kolar

[4] Arnes: Zaščita domačega omrežja (2014), Dostopno na: http://www.arnes.si/pomoc-uporabnikom/varnostna-priporocila/zascita-domacega-omrezja.html#III

[5] Kenneth Ingham, Stephanie Forrest: A history and survey of network firewalls (2002), Dostopno na: http://agl.cs.unm.edu/~treport/tr/02-12/firewall.pdf

[6] Mojca Ciglarič, Zoran Bosnić, James F. Kurose, Keith W. Ross: Računalniške komunikacije, Založba Pearson Education, (2014)

[7] Palo Alto, administracijski priročnik: Threat prevention deployment (2013), Dostopno na: https://live.paloaltonetworks.com/servlet/JiveServlet/previewBody/3094-102-5-15962/Threat%20Prevention%20Deployment%20Tech%20Note%20-%20Version%201.2%20RevA.pdf

[8] Palo Alto, administracijski priročnik: App-ID (2014), Dostopno na: https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/techbrief-app-id.pdf

[9] Uporaba kriptografije v internetu (2007), Dostopno na: http://www.si-ca.si/kripto/kr-osn.htm

[10] Matej Kovačič: Postavitev varnega HTTPS strežnika (2014), Dostopno na: https://pravokator.si/index.php/2014/04/16/postavitev-varnega-https-streznika/

[11] Delovna navodila: Network switching tutorial (2014), Dostopno na: http://www.lantronix.com/resources/net-tutor-switching.html

[12] LAN switching, Dostopno na: http://www.cs.virginia.edu/~itlab/book/pdf/Ch5.pdf

[13] Essentials: Understanding ethernet switches and routers, Volume 3, Issue 1 (2011), Dostopno na: http://www.ccontrols.com/pdf/Essentials0411.pdf

[14] Del Smith CCNA: Understand the evolution of firewalls (2002), Dostopno na: http://www.techrepublic.com/article/understand-the-evolution-of-firewalls/

[15] Wikipedia: Firewall (computing) (2014), Dostopno na: http://en.wikipedia.org/wiki/Firewall_(computing)

[16] Palo Alto, administracijski priročnik: Intrusion Detection System - IDS Technology and Deployment (2014), Dostopno na: https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-detection-system-ids.html

[17] Catherine Paquest, Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide): Network security using cisco ios IPS (2009), Chapter 6, Dostopno na: https://learningnetwork.cisco.com/servlet/JiveServlet/download/6651-1-8391/Ch%25206_Network_Security_Using_Cisco_IOS_IPS.pdf

[18] Suchita Patil, Pallavi Kulkarni, Pradnya Rane, Dr. B.B.Meshram: IDS vs. IPS, International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2, No. 1, (2012), Dostopno na: http://www.ijcnwc.org/papers/vol2no12012/16vol2no1.pdf

[19] Sarah Sorensen: Intrusion detection and prevention (2006), Dostopno na: http://www.cstl.com/Products/Juniper/Juniper-IDP-Solution/WhitePaper/Juniper-IDPWhitePaper.pdf

[20] Palo Alto: User – ID (2014), Dostopno na: https://paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/techbrief-user-id.pdf

[21] Palo Alto: Content – ID: High-Performance Threat Prevention (2014), Dostopno na: https://www.paloaltonetworks.com/products/technologies/content-id.html

[22] Cisco Systems: IP Addressing Guide (2010), Dostopno na: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sba_ipAddr_dg.pdf

[23] Network Address Translation – NAT (2014), Dostopno na: http://www.firewall.cx/networking-topics/network-address-translation-nat.html

[24] Entrust: Understanding Digital Certificates & Secure Sockets Layer (2007), Dostopno na: http://www.entrust.net/ssl-resources/pdf/understanding_ssl.pdf

[25] Blue Coat Systems: Technology primer: Secure Sockets Layer (SSL) (2008), Dostopno na: http://bluecoat.com/documents/download/0485e335-7437-4c4e-bfc0-ca5ffc5bfd4d/16f27cf7-5d59-44b4-b17f-fb04acea369f

[26] Cisco: Next generation encryption (2014), Dostopno na: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

[27] Wikipedia: List of network protocols (osi model) (2014), Dostopno na: http://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model)#Layer_6_protocols_.28Presentation_Layer.29

[28] Palo Alto: Virtualized firewalls, (2014) Dostopno na: https://www.paloaltonetworks.com/products/platforms/virtualized-firewalls/vm-series/overview.html

[29] Himanshu Arora: What is DHCP and How DHCP Works? (2013) Dostopno na: http://www.thegeekstuff.com/2013/03/dhcp-basics/